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

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

ATLAS DATA PRIVACY CORP., AS ASSIGNEE OF INDIVIDUALS WHO ARE COVERED PERSONS; JANE DOE 1, A LAW ENFORCEMENT OFFICER; JANE DOE 2, A LAW ENFORCEMENT OFFICER; EDWIN MALDONADO; SCOTT MALONEY; JUSTYNA MALONEY; PATRICK COLLIGAN; PETER ANDREYEV; AND WILLIAM SULLIVAN,

PLAINTIFFS-APPELLEES,

v.

WE INFORM LLC, ET AL.,

DEFENDANTS-APPELLANTS.

On Appeal from the Order and Memorandum of the United States District Court for the District of New Jersey dated November 26, 2024

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLEES

Alan Butler
Counsel of Record
Megan Iorio
Tom McBrien
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

May 19, 2025

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and 29(c), *amicus curiae* Electronic Privacy Information Center ("EPIC") certifies that it is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

TREATISES

REGULATIONS

INTEREST OF THE AMICUS CURIAE[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC routinely participates as *amicus curiae* in cases concerning privacy rights and the First Amendment implications of data protection regulations. *See* EPIC, *The First Amendment* (2024).[2]

ARGUMENT SUMMARY

Strict scrutiny is the wrong standard by which to evaluate Daniel's Law, especially in a facial challenge posture. The Supreme Court disfavors facial challenges because they "often rest on speculation" and risk short-circuiting democratic processes. Furthermore, as the Court has made clear, the constitutionality of data protection laws, including Daniel's Law, should be

---

[1] All parties consented to the filing of this brief. In accordance with Rule 29(A)(4)(E), the undersigned states that no monetary contributions were made for the preparation or submission of this brief. This brief was not authored, in whole or in part, by counsel for a party.

[2] https://epic.org/issues/platform-accountability-governance/the-first-amendment-and-platform-regulation/.

determined through case-by-case analysis rather than overly broad pronouncements.

Limitations on the disclosure of personal data do not automatically trigger First Amendment scrutiny. *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), held that data regulations implicate the First Amendment when they impose viewpoint discrimination, not that all data dissemination is protected speech. Unlike the law in *Sorrell*, Daniel's Law does not discriminate among favored and disfavored speakers or messages and thus does not burden protected expression in the same way.

Even if the Court finds that Daniel's Law regulates speech, strict scrutiny is inappropriate for evaluating Appellants' facial challenge. Courts overwhelmingly apply intermediate scrutiny to laws limiting the dissemination of personal information, particularly in commercial contexts. Following *Dun & Bradstreet* and its progeny, courts recognize that the commercial exchange of personal data warrants, at most, intermediate scrutiny when it concerns private matters and is motivated solely by profit. This approach has been consistently applied to uphold various data protection laws, including the Fair Credit Reporting Act, Video Privacy Protection Act, and similar statutes.

Appellants' legal theory would render virtually all data protection laws unconstitutional. All such laws necessarily regulate some categories of data and

not others—not as content discrimination, but as appropriate legislative tailoring. Laws like HIPAA, the Video Privacy Protection Act, and the Biometric Information Privacy Act make reasonable distinctions to address specific privacy risks. Subjecting these laws to strict scrutiny would leave Americans defenseless against privacy intrusions and create regulatory chaos across industries.

Given the interlocutory posture of this case following denial of a motion to dismiss, the Court should reject Appellants' facial challenge and remand for further factual and legal development that would enable proper case-by-case analysis of Daniel's Law's constitutionality.

ARGUMENT

I. THE CONSTITUTIONALITY OF DATA PROTECTION LAWS SHOULD BE DECIDED ON A CASE-BY-CASE BASIS.

Supreme Court precedent strongly favors case-by-case review of the constitutionality of statutes, particularly in the privacy context. Appellants' request for sweeping rules that would render all data protection laws presumptively unconstitutional, no matter the factual context in which the law is applied, collides head-on with this precedent.

Facial challenges are generally "disfavored" because they "often rest on speculation" and "threaten to short circuit the democratic process by preventing duly enacted laws from being implemented in constitutional ways." *Moody v. NetChoice,* 603 U.S. 707, 744, 723 (2024) (internal citations omitted). Given the

dangers facial challenges pose, the decision to challenge a statute on its face "comes at a cost." *Id.* at 723. That cost is a heightened evidentiary burden. In the First Amendment context, a court must be able to determine "a law's full set of applications, evaluate which are constitutional and which are not, and compare the one to the other." *Id.* at 718. This includes establishing "what activities, by what actors, the law[] prohibit[s] or otherwise regulate[s]" and "whether there is an intrusion" on protected speech in each application. *Id.* at 724, 708. When a facial challenge is brought against a generally applicable law that has a wide range of applications, such as Daniel's Law, proving facial invalidity can be a "daunting, if not impossible, task." *Id.* at 745 (Barrett, J., concurring).

For this reason, "courts usually handle constitutional claims case by case, not en masse." *Moody,* 603 U.S. at 723. This is especially true in the privacy context, where "the sensitivity and significance of the interests presented in clashes between [the] First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case." *Bartnicki v. Vopper*, 532 U.S. 514, 529 (2001) (quoting *The Florida Star v. B.J.F.*, 491 U.S. 524, 532–33 (1989)). Moreover, "the future may bring scenarios which prudence counsels our not resolving anticipatorily." *Id.; see also id.* at 541 (Breyer, J., concurring) (noting that narrow holdings are necessary in the privacy context because of the need for "legislatures to respond flexibly to the challenges

future technology may pose to the individual's interest in basic personal privacy."). Consequently, the Court has taken pains to "emphasize[] each time that we were resolving this conflict only as it arose in a discrete factual context." *Florida Star*, 491 U.S. at 530.

Tellingly, Defendants rely heavily on cases that resolved as-applied challenges brought by the media or an individual engaged in political speech. *See, e.g., Bartnicki*, 532 U.S.; *Florida Star*, 491 U.S.; *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); *Schrader v. Dist. Att'y of York Cnty.*, 74 F.4th 120, 124 (3d Cir. 2023) (considering only as-applied challenge); *Ostergren v. Cuccinelli*, 615 F.3d 263 (4th Cir. 2010); *Publius v. Boyer-Vine*, 237 F. Supp. 3d 997, 1012 (E.D. Cal. 2017) (limiting analysis to as-applied challenge); or challenges to a statute that narrowly targeted the media, *see, e.g., Smith v. Daily Mail Pub. Co*., 443 U.S. 97, 98 (1979); *Oklahoma Pub. Co. v. Dist. Ct. In & For Oklahoma Cnty.*, 430 U.S. 308 (1977). These as-applied and otherwise narrower challenges, which invalidated laws in specific circumstances involving speech of greater value than most of the speech regulated by Daniel's Law, cannot support facial invalidation here.

II. *SORRELL* ONLY HELD THAT VIEWPOINT-DISCRIMINATORY RESTRICTIONS ON THE FLOW OF INFORMATION TRIGGER FIRST AMENDMENT SCRUTINY.

A law that regulates the dissemination of personal data is not *per se* a regulation of speech under *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011).

The *Sorrell* Court's holding was much more constrained: because personal data can *facilitate* speech, the First Amendment is triggered when the State limits the flow of that data to burden a disfavored message. In other words, the *Sorrell* Court held that regulating the disclosure of personal data implicates the First Amendment when done in a viewpoint-discriminatory way. This is the proper rule to use in applications of Daniel's Law to data brokers, who, at most, facilitate other people's speech by making information available to them. Because Daniel's Law does not discriminate based on viewpoint, it does not implicate the First Amendment as applied to data brokers under *Sorrell*.

The statute at issue in *Sorrell* prohibited the sale and use, for marketing purposes, of data describing physicians' prescribing histories. *Sorrell*, 564 U.S. at 558–59. The law barred pharmaceutical manufacturers and marketers from obtaining and using the data to craft and target their marketing messages, which typically pushed physicians to prescribe brand name drugs. *Id.* at 560–61. But, through a number of exemptions, the law allowed a variety of other persons to obtain and use the data to craft and target their messages, including messages that countered the pharmaceutical manufacturers by promoting generic drugs. *Id.* at 564. The Court observed that the statute "disfavors marketing, that is, speech with a particular content" and further "disfavors specific speakers, namely pharmaceutical manufacturers" and so "on its face [the statute] burdens disfavored

speech by disfavored speakers." *Id.* The legislative history also stated in plain terms that one of the motivations for the statute was that brand-name pharmaceutical marketers "conveyed messages that 'are often in conflict with the goals of the state.'" *Id.* at 565. The Court concluded that the statute was "designed . . . to target [pharmaceutical manufacturers] and their messages for disfavored treatment" in a way that goes "beyond mere content discrimination, to actual viewpoint discrimination." *Id.* (quoting *R.A.V. v. St. Paul,* 505 U.S. 377, 391 (1992)).

In arriving at this conclusion, the Court treated prescriber-identifying data not as speech but as an instrumentality of speech—something that *facilitates* the creation and dissemination of speech. The Court explicitly assumed that the prescriber-identifying information at issue was "a mere commodity" and focused the First Amendment analysis on the burden the state placed on pharmaceutical manufacturer's marketing messages—a well-recognized form of protected commercial speech. *Id.* at 565–66. Because the statute at issue limited the availability of prescriber-identifying information to burden a specific marketing viewpoint, it triggered First Amendment scrutiny.

The analogies the Court made between the regulation of personal data and regulations of news racks and ink help illustrate what it means for personal data to be an instrumentality of speech. *Id.* at 571 ("Vermont's statute could be compared

with a law prohibiting trade magazines from purchasing or using ink."). Like personal data, news racks and ink facilitate the creation and dissemination of speech. But the Court has never held that news racks and ink are speech. Instead, it has held that prohibiting the use of news racks to distribute certain messages and not others, *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 418 (1993), and imposing a tax on ink for some periodicals and not others, *Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue*, 460 U.S. 575 (1983), can trigger First Amendment scrutiny when they amount to viewpoint-based discrimination. *Sorrell*, 564 U.S. at 565–66. The holding of *Sorrell* is that, like news racks and ink, if the state restricts access to personal data in an attempt to burden speech it disagrees with, the state's action is subject to First Amendment review. *See id.* at 571.

The *Sorrell* dicta acknowledged that, sometimes, the dissemination of information can go beyond facilitating speech to being speech itself. Dissemination of information typically becomes speech when the information is part of a larger communication that is itself considered speech under the First Amendment. *Id.* at 570 ("Facts, after all, are the beginning point for much of speech . . ."). For instance, *Bartnicki* concerned a telephone call discussing newsworthy union-related matters. 532 U.S. at 518. There, the "information" was the call itself, "disseminated" as a tape recording to a radio show that played it on air, which is a

paradigmatic example of protected speech. *Id.* at 527. Information on a beer label is commercial speech because companies convey information to consumers on beer labels to inform purchasing decisions, a communication which falls squarely within commercial speech doctrine. *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 481 (1995). But the same information—say, the price of the beer—disclosed to a credit card company to facilitate a purchase is not clearly speech and, instead, more resembles business conduct.

Because data brokers merely facilitate the speech of others, the rule central to *Sorrell*'s holding—and not the rule from the *Sorrell* dicta—is the proper rule to use in applications of Daniel's Law to Appellants. According to their own description of their activities, Appellants "provide contact information for a range of uses central to the economy, political process, and public safety." Appellants' Br. at 15–16 (listing ways others might use the information data brokers disseminate) [hereinafter "Apps' Br.]. That is, Appellants do not themselves engage in speech but, instead make information available to others who, in turn, use this information for their own speech and conduct. Appellants also plainly admit that they are merely *facilitating* other people's speech, not speaking themselves. They say the personal information they disseminate "*facilitates* commerce, political organizing, and public safety," *id.* at 50 (emphasis added) and

"*facilitates* accountability," *id.* at 51 (emphasis added), not that they themselves are engaged in political organizing or accountability work.

Daniel's Law does not implicate the First Amendment under *Sorrell*. Unlike the law at issue in *Sorrell*, Daniel's law does not prohibit the dissemination of information for some messages and not others, nor does it discriminate among favored and disfavored speakers. Daniel's Law thus does not impose content- or viewpoint-based rules on the dissemination of covered person's data and so does not burden protected expression in the way that the law in *Sorrell* did.

III. EVEN IF DISSEMINATION OF DATA IS SPEECH, STRICT SCRUTINY IS INAPPROPRIATE FOR EVALUATING APPELLANTS' FACIAL CHALLENGE.

Even if the dissemination of information is always considered speech, no Court has ever held that the dissemination of personal data is always, or should be assumed to be, *pure* speech that can trigger strict scrutiny. Indeed, Courts overwhelmingly apply intermediate scrutiny to laws that limit the dissemination of personal information unless a specific challenged application involves dissemination of lawfully obtained truthful information of public concern. This is especially the case when the information is exchanged in a commercial context. To analyze Defendants' facial challenge, the Court would need to determine the kind of speech burdened by each application to determine the appropriate level of scrutiny. Defendants have not built a sufficient factual record, nor have they

properly briefed these issues, which means that they cannot succeed in their facial challenge.

A. Courts apply, at most, intermediate scrutiny to laws that regulate the commercial disclosure of personal information.

Courts generally recognize that, to the extent the commercial exchange of personal information implicates the First Amendment, constitutional principles dictate that information be afforded less protection than pure speech. When personal information is not of public concern, its disclosure has not been historically protected to the same extent as personal information of public concern. Further, the very basis of commercial speech scrutiny is the "common-sense" recognition that commercial information is of less value than core speech. *Ohralik v. Ohio State Bar Assn.*, 436 U.S. 447, 455–56 (1978). It thus makes little doctrinal sense to apply strict scrutiny to a regulation of the commercial exchange of personal information.

The Supreme Court "has long recognized that not all speech is of equal First Amendment importance." *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 758 (1985) (plurality opinion). "It is speech on 'matters of public concern' that is 'at the heart of the First Amendment's protection.'" *Id*. at 758–59 (citing *First National Bank of Boston v. Bellotti*, 435 U.S. 765, 776 (1978)). That is because the core aim of the First Amendment is "to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the

people." *New York Times Co. v. Sullivan*, 376 U.S. 254, 269 (1964) (quoting *Roth v. United States*, 354 U.S. 476, 484 (1957)). Thus, when the state seeks to punish those who publish personal information of public importance, there is a "tension between the right which the First Amendment accords to [freedom of speech and of the press], on the one hand, and the protections which various statutes and common-law doctrines accord to personal privacy against the publication of truthful information, on the other." *Florida Star*, 491 U.S. at 530.

While it is often the case that "privacy concerns give way when balanced against the interest in publishing matters of public importance," *Bartnicki*, 532 U.S. at 534, the same cannot be said when the state limits the disclosure of personal data in other circumstances. The common law has long recognized that punishing the improper disclosure of personal information of private concern does not conflict with the First Amendment. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890); *Vidal v. Elster*, 602 U.S. 286, 295–96, 307 (2024) (noting that a restriction on the trademarking of names has long coexisted with the First Amendment, warranting lesser scrutiny). Speech on matters of "purely private concern is of less First Amendment concern" because "[t]here is no threat to the free and robust debate of public issues; there is no potential interference with a meaningful dialogue of ideas concerning self-government; and there is no threat of liability causing a reaction of self-censorship

by the press." *Dun & Bradstreet*, 472 U.S. at 759. To determine whether speech is a matter of public concern, courts look to the "content, form, and context" of the speech "as revealed by the whole record." *Snyder v. Phelps*, 562 U.S. 443, 454 (2011) (quoting *Dun & Bradstreet*, 472 U.S. at 761).

The commercial exchange of personal information receives less protection under the First Amendment both because it is about matters of private concern and because, to the extent that it is speech, it is commercial speech. "Commercial speech, or 'expression related solely to the economic interests of the speaker and its audience,' is ordinarily accorded less First Amendment protection than are other forms of constitutionally guaranteed expression." *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 561 (1980). This is because commercial activity "occurs in an area traditionally subject to government regulation." *Ohralik*, 436 U.S. at 455–456. "[T]he State does not lose its power to regulate commercial activity deemed harmful to the public whenever speech is a component of that activity." *Id*. at 456.

While the "core" of commercial speech doctrine concerns speech that does "no more than propose a commercial transaction," *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 66 (1983), courts have considered this "just a starting point" and "try to give effect to a common-sense distinction between commercial speech and other varieties of speech." *Ariix, LLC v. NutriSearch Corp.*, 985 F.3d 1107,

1115 (9th Cir. 2021). The three *Bolger* factors—whether the speech is an advertisement, whether there is a reference to a specific product, and whether there is an economic motive for disseminating the information—are useful guidance for identifying commercial speech outside the core, but none of the factors are independently necessary or sufficient. *Bolger*, 463 U.S. at 66–67. When the dissemination of personal information is *solely* motivated by profit and has no other expressive purpose, courts have been especially inclined to find that commercial speech scrutiny applies. *See, e.g., Dun & Bradstreet*, 472 U.S. at 762; *Stark v. Patreon*, 656 F. Supp. 3d 1018, 1034 (2023); *King v. Gen. Info. Servs., Inc.*, 903 F. Supp. 2d 303, 307 (E.D. Pa. 2012).

When considering the proper level of scrutiny for laws that regulate the commercial dissemination of personal information, courts have taken a "wholistic approach" that combines the public vs. private concern inquiry with the considerations underlying the commercial speech doctrine. *Stark*, 656 F.Supp.3d at 1033–34. This approach has its roots in the Supreme Court's plurality opinion in *Dun & Bradstreet v. Greenmoss Builders*, which was decided two years after *Bolger*. 472 U.S. at 759.[3] In *Dun & Bradstreet*, the Court applied commercial

[3] Even before *Dun & Bradstreet*, two circuit courts had found that regulations of credit reporting were subject to commercial speech scrutiny. *See Millstone v.*

speech doctrine to a defamation claim involving a false business credit report. The plurality noted that the speech at issue was of private concern because distribution was limited to a small group of subscribers, the information was "solely in the individual interest of the speaker and its specific business audience" and there was "simply no credible argument that this type of credit reporting requires special protection to ensure that debate on public issues will be uninhibited, robust, and wide-open." *Id.* at 762 (citation and quotation marks omitted). The plurality also observed that, like advertising, credit reporting "is hardy and unlikely to be deterred by incidental state regulation" because it is "solely motivated by the desire for profit." *Id*. (citing *Virginia Pharmacy Bd. v. Virginia Citizens Consumer Council, Inc.*, 425 U.S., at 771–772). The two justices whose concurrences were necessary to form a majority agreed that credit reports were information of private concern and neither disagreed with the application of commercial scrutiny in this context. *See id.* at 763–64; (Burger, J., concurring); *id.* at 765–74 (White, J., concurring).

Following *Dun & Bradstreet*, courts have used the same reasoning to reject, under commercial speech scrutiny, First Amendment challenges to the Fair Credit

---

O'Hanlon Reps., Inc., 528 F.2d 829, 833 (8th Cir. 1976); *Hood v. Dun & Bradstreet, Inc.*, 486 F.2d 25, 30 (5th Cir. 1973).

Reporting Act ("FCRA"), which regulates the disclosure of personal information in credit reporting. In *Trans Union v. FTC*, for instance, the D.C. Circuit rejected Trans Union's challenge to the FCRA's limit on the dissemination of financial information for targeted marketing. 267 F.3d 1138 (D.C. Cir. 2001). The court found that, as in *Dun & Bradstreet*, targeted marketing lists are purchased through a subscription model and interest only "the speaker (Trans Union) and its specific business audience (its customers)." *Id.* at 1140 (internal quotation marks and citation omitted). Moreover, the D.C. Circuit found that Transunion's target marketing lists, which included people's names, addresses, and financial circumstances, were "speech of purely private concern"—even more so than the credit report in *Dun & Bradstreet* because they contained the personal information of individuals, not corporations. *Id*. A district court in this circuit similarly rejected a First Amendment challenge to one of the FCRA's disclosure limitations, applying commercial speech scrutiny because the consumer reporting agency disseminated information "for the purpose of making a profit," its business subscribers used the information "to make business decisions," and so the information was "of sole interest to the speaker (GIS) and its audience (business customers)" and did "not significantly contribute to public dialogue." *King*, 903 F. Supp. 2d at 307.

Courts around the country have recognized that similar reasoning as that in *Dun & Bradstreet* and *Trans Union* justifies applying, at most, commercial speech scrutiny in First Amendment challenges to laws that limit the commercial disclosure of personal information. *See Khimmat v. Weltman, Weinberg & Reis Co., LPA*, 585 F. Supp. 3d 707, 715 (E.D. Pa. 2022) (upholding a provision of the Fair Debt Collection Practices Act under commercial speech doctrine); *Jackin v. Enhanced Recovery Co., LLC*, 606 F. Supp. 3d 1031, 1039 (E.D. Wash. 2022) (same); *ACA Connects - Am.'s Commc'ns Ass'n v. Frey*, 471 F. Supp. 3d 318, 327 (D. Me. 2020) (upholding Maine online privacy law under commercial speech doctrine); *Saunders v. Hearst Television, Inc.*, 711 F. Supp. 3d 24, 32–33 (D. Mass. 2024) (upholding federal Video Privacy Protection Act under commercial speech doctrine); *Christopherson v. Cinema Ent. Corp.*, No. 23-CV-3614 (JWB/LIB), 2024 WL 1120925 (D. Minn. Mar. 6, 2024) (same). In upholding the Michigan Video Rental Privacy Act, which limits the disclosure of consumers' video viewing habits, a court noted that the state should "be afforded greater leeway in regulating the dissemination of consumer data" because this information "concerns strictly private affairs" and "the economic motive driving the disclosure of consumer identifying information makes the speech more 'durable' and less likely to be deterred by government regulation." *Boelter v. Hearst Commc'ns, Inc.*, 192 F. Supp. 3d 427, 446 (S.D.N.Y. 2016). And in upholding the equivalent

federal statute, the Video Privacy Protection Act, under commercial speech doctrine, a court noted that the disclosure of personal data was "motivated by commercial interests," had "no expressive or creative content beyond the fact of Plaintiff's personal information and interactions" with the website, "contain[ed] nothing of public interest," and "serv[ed] no non-economic purpose to either the speaker or the recipient." *Stark*, 656 F. Supp. 3d at 1034.

Where a data protection law limits the commercial disclosure of personal information, it does not matter whether the law is purportedly content-based; strict scrutiny simply does not apply. "The Supreme Court has consistently applied intermediate scrutiny to commercial speech restrictions, even those that were content- and speaker-based." *Greater Philadelphia Chamber of Com. v. City of Philadelphia*, 949 F.3d 116, 138 (3d Cir. 2020) (gathering cases). Even outside the commercial speech context, unless a restriction "raises the specter that the Government may effectively drive certain ideas or viewpoints from the marketplace," strict scrutiny is inappropriate. *R.A.V.*, 505 U.S. at 387–88. *See also Greater Philadelphia Chamber of Com.*, 949 F.3d at 139. For this reason, courts have rejected the idea that data protection laws are content-based and subject to strict scrutiny merely because they regulate some categories of data and not others. *See Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 949 (7th Cir. 2015)

(Driver's Privacy Protection Act); *Sosa v. Onfido, Inc.*, 600 F. Supp. 3d 859, 880 (N.D. Ill. 2022) (Illinois's Biometric Information Privacy Act).

B. Strict scrutiny is inappropriate in all but a few hypothetical applications of Daniel's Law.

Facial challenges cannot be resolved based on vague doctrinal hand-waving. The Court must look at each application of the law and decide whether it is constitutional; it must then weigh the unconstitutional applications against the constitutional ones. *Moody*, 603 U.S. at 744. Appellants have failed to analyze *any* concrete application of Daniel's Law, let alone all of them. For that reason alone, this Court lacks a sufficient record to grant Appellants' facial challenge.

What's more, Appellants would likely have difficulty proving their facial challenge even with a fully developed record. The application of Daniel's Law to the Appellants themselves would most likely call for intermediate scrutiny because it is both speech on matters of private concern and commercial speech. Daniel's Law regulates the dissemination of individual's names, addresses, and phone numbers—which, when sold to a limited audience, is "speech of purely private concern." *Trans Union*, 267 F.3d at 1140. The sale of public officials' home addresses and phone numbers generally "do[es] nothing to inform the public about any aspect of [government] functioning or operation" and does not "relat[e] to any matter of political, social, or other concern to the community." *Snyder*, 562 U.S. at 453. Data brokers are also "solely motivated by the desire for profit," *Dun &*

Bradstreet, 472 U.S. at 762, and the sale of data has "no expressive or creative content beyond the fact of [covered persons'] personal information," *Stark*, 656 F. Supp. 3d at 1034. The commercial sale of home addresses and phone numbers is thus "hardy and unlikely to be deterred" by regulation, *Dun & Bradstreet*, 472 U.S. at 762, and of lesser value than core First Amendment speech. It does not warrant the same level of scrutiny as core First Amendment speech.

Other commercial applications of Daniel's Law should also receive, at most, commercial speech scrutiny. Application of Daniel's Law to credit reporting would clearly warrant, at most, commercial scrutiny under *Dun & Bradstreet* and *Trans Union*, as would other examples of business-to-business disclosures of personal information. To protect the disclosure of personal information used to facilitate commercial speech (e.g., targeted marketing lists) to a greater extent than the commercial speech itself, as Appellants suggest, rankles "common-sense," particularly because this information has no public significance. *See Ohralik*, 436 U.S. at 455–456.

In any event, as a generally applicable regulation, Daniel's Law applies to a wide range of people and companies—far more than the few examples Appellants provided in their brief. *See* Apps' Br. at 15–16 (listing eight contexts in which Daniel's Law applies). On this record, the court is not able to determine the full

range of application of Daniel's Law, let alone determine what level of scrutiny is appropriate in each.

Even in hypothetical applications of Daniel's Law to disclosures made by the media or for political purposes, it is not at all clear that the law would be unconstitutional. Indeed, a state appellate court last year rejected an as-applied challenge to Daniel's Law involving a journalist reporting on a matter of public concern. *Kratovil v. City of New Brunswick*, No. A-0216-23, 2024 WL 1826867 (N.J. Super. Ct. App. Div. Apr. 26, 2024), *pet. for review granted,* 258 N.J. 468 (Sep. 20, 2024). The court found that the disclosure of a public official's complete address was unnecessary to report the matter of public interest, and that disclosure of the town alone would have been sufficient to fully report the newsworthy information: that the official resided hours away from the town where they held office. *Id.* at *5–6.

Considering that this case is before the Court on interlocutory appeal following a denial of a motion to dismiss, it is appropriate for the Court to deny Defendants' facial challenge and send the case back to the district court for further factual and legal development.

IV. THE APPELLANTS' LEGAL THEORY WOULD RENDER VIRTUALLY EVERY DATA PROTECTION REGULATION UNCONSTITUTIONAL.

A. All data protection laws regulate some categories of personal data and not others.

If any data protection law that singles out specific data categories for regulation is "content-based" and requires strict scrutiny, then virtually all data protection laws are presumptively unconstitutional because they all regulate some data (e.g., personal data) and not other data (e.g., price information). There must be a distinction between highly suspect content discrimination and appropriate legislative tailoring. Otherwise, legislators face an impossible choice: regulate all data at once and in an identical way, or do not regulate data at all.

Even the broadest comprehensive privacy laws regulate some but not all data disclosures. For example, the California Consumer Privacy Act (CCPA) regulates personal information but not scientific or corporate information. *See* Cal. Civ. Code § 1798.140(v)(1). Comprehensive data protection laws also regulate some categories of personal data differently than others. The CCPA regulates the disclosure of "sensitive personal information" more tightly than other types of personal information. *Compare* Cal. Civ. Code § 1798.120, *and* Cal Civ. Code § 1798.121. These reasonable distinctions and boundaries cannot mean a law is facially content-based and presumptively unconstitutional.

Important sectoral privacy laws would be even more vulnerable under the Appellants' theory. The Health Insurance Portability and Accountability Act (HIPAA) only regulates disclosure of protected health information. 45 C.F.R. § 160.103 (2024). The Video Privacy Protection Act (VPPA) only regulates disclosure of video viewing history. 18 U.S.C. § 2710(a)(3). The Biometric Information Privacy Act (BIPA) only limits disclosure of biometric identifiers and related information. 740 Ill. Comp. Stat. 14/10 (2008). Even the nearly 150-year-old misappropriation tort only regulates use of names and likenesses. *See* Restatement (Second) of Torts § 652C (1977); Jennifer Rothman, The Right to Publicity 20 (2018) (describing an 1890 New York case involving the misappropriation tort). So would laws that have been proposed to combat some of the most egregious privacy invasions of new technology, like the unfettered dissemination of people's granular location data. *See, e.g.*, A.B. 1355, 2025-2026 Reg. Sess. (Cal. 2025) (amending the CCPA to add precise geolocation to the definition of "sensitive personal information").

Data protection laws regulate some but not all data in order to address risks arising from specific data disclosures. For example, HIPAA protects personal health data to preserve individual privacy in sensitive health information and to promote trust in the healthcare system. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82465–66 (Dec. 28, 2000) (to be

codified at 45 C.F.R. pts. 160, 164). Strangers and hostile personal contacts should not be able to access sensitive details like pregnancy information, cancer diagnoses, or hair loss treatments. HIPAA's disclosure limits also maintain trust in the healthcare system by enforcing patient-doctor confidentiality. By ensuring that patients are comfortable providing accurate medical information to their doctors, HIPAA facilitates quality medical treatment and enables useful public health research that depends on accurate information. *Id.* at 82466.

HIPAA's content-specificity represents a natural means-ends fit. HIPAA does not regulate disclosure of a patient's salary or video-watching preferences because that would not further its medical privacy goals. Similarly, if HIPAA did not specifically regulate *identifiable* personal health information, then it would prevent disclosure of de-identified health information that is crucial for scientific research. This content-specificity serves important goals in a reasonable way.

Nearly all data protection laws follow this pattern, reflecting proper boundary-drawing instead of a widespread censorship scheme. The Video Privacy Protection Act regulates video viewing records to safeguard the constitutional freedoms of opinion and association. S. Rep. No. 100-599, at 7 (1988). Congress's reasonable decision not to have the VPPA cover information a video-hosting platform would likely never have, such as users' tax forms, should not result in strict scrutiny being applied. A similar analysis would apply to the Fair Credit

Reporting Act's (FCRA) protections for information related to credit reports, 15 U.S.C. § 1681 *et seq.*, and the Graham-Leach Bliley Act's (GLBA) privacy protections for financial data, 15 U.S.C. §§ 6801–6809.

Courts have consistently indicated that reasonably content-specific data protection laws are not the same as suspiciously content-based ones. The Supreme Court remarked that HIPAA's content-specificity was a constitutional *advantage*, not a pitfall, because the "[s]tate . . . advanced its asserted privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances." *Sorrell*, 564 U.S. at 573. In *Vidal v. Elster*, the Supreme Court granted unanimous approval to the Lanham Act's "names clause," a content-based provision similar to the misappropriation tort. While the fractured opinion involved four separate modes of analysis, none of them applied strict scrutiny. *See generally Vidal v. Elster*, 602 U.S. 286 (2024). The VPPA and BIPA have also been upheld under intermediate, not strict, scrutiny. *See Stark*, 656 F. Supp. 3d at 1034 (VPPA); *Sosa*, 600 F. Supp. 3d at 880 (BIPA); *In re Clearview AI, Inc., Consumer Priv. Litig.*, 585 F. Supp. 3d 1111, 1120 (N.D. Ill. 2022) (BIPA).

In sum, data protection laws support a variety of foundational rights and interests. To do so in an appropriately tailored and effective way, these laws regulate dissemination of specific categories and sources of information. Holding that this means they are content-based restrictions on speech that are presumptively

unconstitutional would be dangerously overbroad and, if adopted widely, would threaten the many interests described above.

B. Appellants' theory, if adopted widely, would threaten to destroy the entire regime of data protection.

Under the withering gaze of strict scrutiny, any data protection law can be styled as over- or under-inclusive and ruled unconstitutional. Given the scale and complexity of the modern economy and the internet, even the most carefully drawn privacy laws are vulnerable to over- and under-inclusiveness arguments. Inappropriately subjecting every data protection regulation to strict scrutiny would leave Americans virtually defenseless against privacy intrusions and create regulatory chaos across industries. Such an interpretation cannot stand under established constitutional principles.

Data protection laws necessarily involve over- or under-inclusive regulation of data flows based on their need to balance competing interests, not based on an intent to burden a certain viewpoint or topic. Data protection laws implicate tradeoffs among many important values: specificity, clarity, ease of compliance, protectiveness, resilience to changing technology, and more. Requiring a best fit instead of a merely reasonable one opens up data protection laws to endless constitutional nitpicking that would make data protection impossible to legislate and enforce.

Subjecting a law like HIPAA to strict scrutiny underscores the need for judicial caution in extending strict scrutiny beyond its proper scope. It is facile to identify slight instances of over-inclusiveness in HIPAA. The law, for example, treats disclosure about a routine physical the same as disclosure of an HIV diagnosis. 45 C.F.R. § 160.103 (2024). One could easily cast this as failing a least restrictive means analysis under strict scrutiny. But imagine requiring healthcare workers to sort personal health information into numerous sensitivity categories, each with its own disclosure rules. It would be a compliance nightmare and make serious mistakes inevitable. HIPAA, while potentially over-inclusive in some respects, represents a reasonable attempt to balance patient privacy with ease of compliance for healthcare workers and peace of mind for patients.

Similarly, HIPAA can easily be cast as unconstitutionally under-inclusive because it does not regulate every entity that holds personal health information. Its list of covered entities includes health plans, health care clearinghouses, and health care providers who electronically transmit any health information. 45 C.F.R. § 160.103 (2024). This excludes many entities that also hold sensitive personal health information such as health and wellness apps, search engine companies, data brokers, social media platforms, and more. While worth amending, these gaps simply represent the fact that non-covered entities did not exist at the time the Department of Health & Human Services promulgated HIPAA's Privacy Rule, not

an intent to restrict hospitals' and insurers' speech and elevate that of wellness apps. And even if these gaps were fixed, HIPAA would still under-inclusively "discriminate" based on speaker since the law would never be amended to punish one's spouse for mentioning to one's mother that one had a headache last weekend without formal written consent.

The same needlessly restrictive analysis could apply to virtually any data protection law. The VPPA's protection of intellectual privacy is under-inclusive because it protects video-watching habits but not reading habits, both of which are highly indicative of a person's viewpoints. *See* Neil Richards, *Intellectual Privacy*, 87 Texas L. Rev. 387, 441 (2008). This reflects the fact that VPPA was passed in response to a highly public violation of a Supreme Court Justice nominee's video viewing history, *Developments in the Law — More Data, More Problems*, 131 Harv. L. Rev. 1715, 1722 (2018), not an effort to silence Netflix in favor of Barnes & Noble. The VPPA could simultaneously be labeled over-inclusive because it treats the disclosure of a person's rental of pornography and nature documentaries the same. *See* 18 U.S.C. § 2710(c).

Applying strict scrutiny in this way to all data protection laws would send the entire regime of data protection on a race to the bottom. Companies that desire deregulation to maximize their profits will push for the lightest-touch regulation, or none whatsoever, as the least restrictive means. A law that prohibits disclosure of

personal information might be overturned for not instead allowing users to opt in to disclosure. A law that allows users to opt in might be overturned for not using an opt-out scheme. And a law that uses and opt-out scheme might be challenged for limiting disclosure at all instead of merely educating users about privacy risks or a vague notion that hypothetical privacy-protective tools would do the job. The end result would be the end of privacy law as we know it.

The Appellants' legal theories cut against history, tradition, common sense, and Supreme Court caselaw, all of which counsel that data protection laws may coexist with the First Amendment. This Court's ruling should be careful not to upend the entire edifice of data protection but, instead, reserve strict scrutiny for laws that actually threaten speech.

CONCLUSION

Amicus respectfully request this Court affirm the lower court's order granting Appellee's motion to dismiss.

*/s/ Alan Butler*_____
Alan Butler
Counsel of Record
Megan Iorio
Tom McBrien
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
butler@epic.org