William & Mary Law Review

Volume 64 (2022-2023)
Issue 1

Article 5

10-2022

Preempting the States and Protecting the Charities: A Case for Nonprofit-Exempting Federal Action in Consumer Data Privacy

Sarah Fisher

NOTES

PREEMPTING THE STATES AND PROTECTING THE CHARITIES: A CASE FOR NONPROFIT-EXEMPTING FEDERAL ACTION IN CONSUMER DATA PRIVACY

TABLE OF CONTENTS

INTRODUCTION

Imagine the following: residents of Smalltown, Virginia, a community transitioning away from coal production and toward green fuels, become interested in educating their neighboring cities and counties about the environmental benefits of sustainable energy production.[1] Familiar with national nonprofit groups founded to educate the public on environmental causes and green energy, Smalltowners run a quick internet search and discover that no such organizations exist in their corner of the Commonwealth.[2] Thus, at a local government meeting, the Smalltowners decide to create their own educational, charitable organization to teach their peers about the environmental benefits of sustainable fuels and to raise funds for those impacted by coal-related health conditions.

Pro bono Smalltown Lawyer recommends that the Smalltowners create an entity under Virginia law and has Smalltown Paralegal file articles of incorporation to form a nonstock corporation.[3] After official formation of the new organization, Smalltown Charity applies for and receives federal tax-exempt status from the Internal Revenue Service under section 501(c)(3) by virtue of the group's charitable and educational mission.[4] Smalltown Charity promptly

---

1. This premise is hypothesized from the transition away from coal production happening across the Appalachian region of the United States. *See* Abby Neal, *Issue Brief: How Coal Country Can Adapt to the Energy Transition*, ENV'T & ENERGY STUDY INST. (Nov. 10, 2020), https://www.eesi.org/papers/view/issue-brief-how-coal-country-can-adapt-to-the-energy-transition [https://perma.cc/UEY3-JY57] (describing general framework of transition from coal to renewable energy in America).

2. *See, e.g.*, *Mission & History*, ACORE: AM. COUNCIL ON RENEWABLE ENERGY (2021), https://acore.org/mission-history/ [https://perma.cc/7T5T-R9Q9].

3. *See* Virginia Nonstock Corporation Act, VA. CODE ANN. §§ 13.1-800 to -945 (2020) (establishing procedure for forming nonstock corporation); *see also FAQs - Virginia Nonstock Corporations (Including Nonprofits)*, STATE CORP. COMM'N (2021), https://www.scc.virginia.gov/pages/Virginia-Nonstock-Corporations-FAQs [https://perma.cc/73E8-DVEQ] (explaining that under Virginia law, nonstock corporations are often formed for "non-profit purposes, such as ... charitable organizations").

4. I.R.C. § 501(c)(3). Note that the process for applying for federal tax-exemption under section 501(c)(3) has been substantially simplified with the introduction of IRS Form 1023-EZ, Streamlined Application for Recognition of Exemption. As such, obtaining tax-exemption is often feasible without legal assistance. *See Streamlined Application for Recognition of Exemption Under Section 501(c)(3) of the Internal Revenue Code*, IRS (June 7, 2021), https://www.irs.gov/forms-pubs/about-form-1023-ez [https://perma.cc/6LH4-PBCQ].

begins soliciting and receiving donations from Virginians and soon produces a series of environmental education videos that go viral online with a creative hashtag.[5] Smalltown Charity receives a tidal wave of interested donors from Virginia who are beyond eager to support the group's cause. Unconvinced that Smalltown Charity's popularity will continue and unable to purchase expensive record-keeping systems, the Smalltowners' cause remains an all-volunteer operation with donation information recorded in basic software.[6]

One year after the viral campaign, Smalltown Charity receives an email from Bigtown Donor demanding that Charity delete any information it has on file about him and alleging that Charity has failed to gain his consent for using his information in targeted educational mailing materials.[7] Donor claims that a new Virginia data privacy law gives him rights to these actions and requires Charity to set up sophisticated processing systems to constantly monitor donor information.[8] Smalltown Charity finds the new law online and rushes to contact Smalltown Lawyer to interpret the statute. Lawyer declines to provide additional pro bono services, leaving Charity's volunteers to interpret the legalese of a 6,000-word statute on their own.[9]

Through the volunteers' informal research, Charity discovers that new, similar data privacy measures have also been passed in California, Colorado, and the European Union.[10] Smalltown volunteers

---

5. *See, e.g.*, Brian Frederick, *Ice Bucket Challenge Dramatically Accelerated the Fight Against ALS*, ALS ASS'N (June 4, 2019), https://www.als.org/stories-news/ice-bucket-challenge-dramatically-accelerated-fight-against-als [https://perma.cc/D8JT-W3LZ] (example of viral nonprofit educational and marketing campaign).

6. *See* Brice S. McKeever, *The Nonprofit Sector in Brief 2018: Public Charities, Giving, and Volunteering*, THE URBAN INST. (Nov. 2018), https://nccs.urban.org/publication/nonprofit-sector-brief-2018#the-nonprofit-sector-in-brief-2018-public-charities-giving-and-volunteering [https://perma.cc/72SP-ZCP6] (noting "over two-fifths of public charities rely on volunteers").

7. It is common for tax-exempt and other nonprofit organizations to use donor demographic data in creating effective solicitation materials. *See, e.g.*, *Industries-Non-Profit & Charity*, SPECTRUM MKTG. COS. (2021), https://spectrummarketing.com/industries/non-profit-direct-mail/ [https://perma.cc/9U5S-FNMS] (providing example of marketing firm providing data-driven direct mail services to nonprofits).

8. See Virginia Consumer Data Protection Act (VCDPA), VA. CODE ANN. §§ 59.1-575 to -585 (2021) (effective Jan. 1, 2023) for the measure alluded to in this scenario.

9. *See id.*

10. *See* California Consumer Privacy Act (CCPA), CAL. CIV. CODE §§ 1798.100-.199.100 (West 2023) (effective Jan. 1, 2023); Colorado Privacy Act (CPA), 2021 Colo. Sess. Laws 3445, 3448 (to be codified at COLO. REV. STAT. §§ 6-1-1301 to -1313) (effective July 1, 2023);

skim the Charity's records and discover that the Charity has received donations from donors in all three of these jurisdictions. Mistakenly believing that the receipt of a singular donation is a sufficient trigger for requiring compliance with each of these measures, Smalltown Charity scrambles to upgrade its software and takes out loans to retain a data protection firm and a privacy attorney from neighboring Bigtown. Eventually, Smalltown Charity is forced into bankruptcy, driven out of operation by the sky-high compliance costs incurred by an inaccurate reading of complex privacy statutes.[11]

This scenario highlights the two most significant challenges posed by the emerging patchwork of consumer privacy and data protection statutes to nonprofit organizations. First, nonprofit organizations—particularly 501(c)(3) tax-exempt groups—uniquely *rely* on personal data in the form of donations to power their budgets and their programs and thus are uniquely *overburdened* by statutes that demand overhauls to internal personal data processing systems.[12] 501(c)(3) charitable and educational organizations are sustained by the dollars of their donors, dollars that are processed alongside personal information that is, in turn, used for targeted

---

Commission Regulation 2016/679 of Apr. 27, 2016, The Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

11. While this scenario is dramatized, the compliance costs for a tax-exempt organization seeking to conform with any one of these measures can be astronomical. For example, a data review conducted by cybersecurity and privacy publication *CPO Magazine* found that 34 percent of small- and mid-sized organizations spent between $100,000 and $499,000 on complying with the GDPR. Notably, the Magazine concluded that "[o]nly 6% of all organizations spent less than $50,000." Nicole Lindsey, *Understanding the GDPR Cost of Continuous Compliance*, CPO MAG. (May 31, 2019), https://www.cpomagazine.com/data-protection/understanding-the-gdpr-cost-of-continuous-compliance/ [https://perma.cc/H6H5-XQAF]. When considering that nearly 40 percent of section 501(c)(3)-exempt organizations filing with IRS for fiscal year 2018 reported $500,000 or fewer in assets—and that nearly 15 percent reported an asset value under $100,000—privacy compliance costs can easily drive tax-exempt organizations out of operation. *See* INTERNAL REVENUE SERV., FORM 990 RETURNS OF 501(C)(3) ORGANIZATIONS: BALANCE SHEET AND INCOME STATEMENT ITEMS, BY ASSET SIZE, TAX YEAR 2018 (2019), https://www.irs.gov/statistics/soi-tax-stats-charities-and-other-tax-exempt-organizations-statistics [https://perma.cc/AWT6-UCBJ].

12. For 501(c)(3) organizations reporting under $500,000 in assets for FY2018, roughly 53 percent of revenue came from contributions, gifts, and grants. *See* INTERNAL REVENUE SERV., *supra* note 11.

programming.[13] Second, the costs of compliance relative to income are higher for tax-exempt organizations by virtue of their limited budgets and personnel resources.[14] These costs are applicable to organizations that incorrectly conclude compliance is required as well as organizations that accurately assess their compliance obligations.[15]

Perhaps in recognition of these difficulties, select enacted data privacy protection measures explicitly exempt 501(c)(3) organizations from compliance.[16] The European Union's GDPR requires compliance from any entities that process the "personal data" of individuals located in the EU, with "personal data" broadly defined as "any information relating to an ... identifiable natural person."[17] The GDPR does not distinguish between data captured for for-profit purposes versus data used in nonprofit ventures.[18] By contrast, California's CCPA generally applies only to for-profit entities but can capture nonprofits in the compliance net depending on the details of their business relationships with for-profit entities, such as sharing corporate branding.[19] Colorado's CPA measure mirrors the GDPR in failing to exempt any nonprofits from compliance,[20] while Virginia's VCDPA exempts only Virginia-formed nonstock

13. *See id.*; *see also* SPECTRUM MKTG. COS., *supra* note 7; *Donating to Charity*, USAGOV (2021), https://www.usa.gov/donate-to-charity [https://perma.cc/4RFG-NDKU] (noting that donors are often able to take federal tax deductions for donations to 501(c)(3) organizations). The ability to claim a deduction makes donation to a recognized 501(c)(3) organization more appealing when compared to other classifications of nonprofit or tax-exempt organizations.

14. Compliance costs for tax-exempts in this space come in two flavors. The first captures upfront costs associated with determining if compliance is even required. Smalltown Charity was unable to withstand this cost, leading to Charity's reliance on lay volunteers who incorrectly interpreted lengthy statutes and prompting unnecessary spending under the color of compliance. The second includes ongoing, genuine compliance costs associated with maintaining the systems and protocols required under the various measures. *See, e.g.*, Lindsey, *supra* note 11.

15. *See supra* note 14 and accompanying text.

16. *See, e.g.*, VA. CODE ANN. § 59.1-575 (2021) (defining "nonprofit organization" to include organizations exempt under I.R.C. § 501(c)(3) and stating that the provisions of the VCDPA "shall not apply to any ... nonprofit organization"). *But see* COLO. REV. STAT. § 6-1-1304(2) (effective July 1, 2023) (exempting certain entities such as healthcare facilities and airlines from compliance with the CPA but failing to exempt any classifications of nonprofit organizations).

17. GDPR, *supra* note 10, at art. 4(1).

18. *See id.* at art. 2(1)-(4).

19. CAL. CIV. CODE § 1798.140(c)(2) (West 2023).

20. COLO. REV. STAT. § 6-1-1304(2).

corporations and Internal Revenue Service (IRS)-classified 501(c)(3) organizations.[21]

This confusing patchwork of state and international measures, coupled with the internet-age phenomenon of even tiny organizations processing data from donors around the globe, presents 501(c)(3) groups with a Morton's fork: either to risk bankruptcy by expending the massive monetary and temporal resources necessary to determine compliance and overhaul internal systems or to do nothing and risk disciplinary action for failure to comply with any one of these measures.[22] Both types of risk carry heightened societal consequences as both endanger organizational bankruptcy. As a public policy matter, 501(c)(3) classification exists on the theory that (c)(3) organizations offer societal benefits so significant that the government is willing to subsidize said organizations' operations by virtue of federal tax-exemption.[23] Simultaneously, widespread compliance with some set of consumer data privacy standards is crucial for vindicating the individual privacy interest central to existing data privacy law.[24]

Preferably, then, the optimal consumer data privacy scheme is one that would balance the interests of individual consumers in controlling their personal information online against the collective, societal interest of 501(c)(3) organizations' continued operation.[25] The ideal arrangement would also eliminate the confusing patchwork system of disparate, single-jurisdiction measures currently in place in favor of a uniform, singular standard operative nationwide.[26]

---

21. VA. CODE ANN. § 59.1-576.

22. *See supra* notes 11-21 and accompanying text.

23. *See* Nicholas A. Mirkay, *Is It "Charitable" to Discriminate?: The Necessary Transformation of Section 501(c)(3) into the Gold Standard for Charities*, 2007 WIS. L. REV. 45, 86 (2007) (stating that "[c]haritable exemptions are justified on the basis that the exempt entity confers a public benefit—a benefit which the society or the community may not itself choose or be able to provide, or which supplements and advances the work of public institutions" (quoting Bob Jones Univ. v. United States, 461 U.S. 574, 591-92 (1983))).

24. *See, e.g.*, Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 83 (2018) (noting, in a discussion of privacy law in the United States and Europe, that the "European focus has traditionally been first and foremost on individual privacy protection as a basic human right" (internal quotations and citation omitted)).

25. *See infra* Part III.

26. *See infra* Part III.

How does such an ideal system emerge? This Note argues that Congress should use its Commerce Clause power to pass a consumer data privacy measure that (1) preempts state law and (2) explicitly exempts 501(c)(3) organizations from compliance.[27] Such preemptive action with a narrow 501(c)(3) carve-out would avoid the potential harm of exempting too broad a group of nonprofit entities while ensuring charitable organizations' continued existence, would be more protective of both the individual privacy right and 501(c)(3) existence than merely adjusting the revenue dollar threshold at which entities must comply, and would properly balance the individual right to control personal data with the societal good served by the existence of 501(c)(3) charitable organizations.[28]

Part I of this Note elaborates on the relationship between 501(c)(3) organizations and personal data and expands on the compliance difficulties faced by (and the collective societal good of) (c)(3) groups. Part II reviews the four major existing privacy law measures—the GDPR, the CCPA, the CPA, and the VCDPA—and analyzes the scope of each measure's reach as it pertains to 501(c)(3) charities. Part III of this Note makes the case for federal preemptory action in a sweeping consumer privacy rights measure that trumps the existing patchwork of state law and exempts 501(c)(3) organizations from compliance. Finally, Part IV of this Note considers and responds to potential Tenth Amendment and state expertise counterarguments that could be raised in opposition to federal preemptory action in this arena.

I. 501(C)(3) DATA USE BACKGROUND

An overview of the centrality of data to 501(c)(3) organizations' operations is necessary to ground the discussion in Parts II, III, and IV of this Note.

For-profit businesses, especially those with expansive online presences, often have entire revenue and expense streams dedicated to the purchase and sale of consumer data.[29] The rise of "big data"

---

27. *See infra* Part III.

28. *See infra* Part III.

29. *See Benefits of Big Data: Increased Revenues and Reduced Costs*, BUS. APPLICATION RSCH. CTR. (2019), https://bi-survey.com/big-data-benefits [https://perma.cc/XF4N-Q5K7] (de-

is no doubt a market-wide phenomenon,[30] yet 501(c)(3) organizations' use of and reliance on consumer data differs meaningfully from that of their for-profit counterparts. First, charitable organizations *must* collect personal data—often copious amounts of it—because they are funded predominantly by natural-person donations.[31] Second, 501(c)(3) exempt organizations' programmatic activities often utilize donor and member data for successful operations.[32] Consumer data is used to solicit new donors, to identify potential new members to join the organization, to target possible volunteers, to direct communications and programs towards those most likely to participate, and to coordinate activities with related and like-minded organizations.[33] By virtue of their tax-exempt classification, 501(c)(3) organizations often have "people" at the heart of their exempt purpose: two central permissible purposes under section 501(c)(3) are charitable and educational missions,

---

scribing results from big data use study and concluding big data is responsible for 8 percent increase in revenue and 10 percent reduction in costs for for-profit entities worldwide, with a key benefit found in "a better understanding of customers").

30. *See id.*

31. This reliance on donor-consumer data is driven by IRS regulations surrounding section 501(c)(3) exemption. To maintain exempt status under (c)(3), an entity must typically demonstrate that it meets the "public support test," *see* 26 C.F.R. § 1.170A-9(f)(4)(v) (2020), a regulatory standard that requires 501(c)(3) organizations to show they have a wide variety of funding from "public" sources (namely, natural persons and other public charities). *See id.* § 1.170A-9(f)(3)(iii)(B). This test has slight variations depending on the subclassification sought by the (c)(3) entity, but broadly speaking, organizations must demonstrate a public support percentage of at least 33.3 percent over a five-year cumulative basis to continue to receive federal tax-exemption. *See id.* § 1.170A-9(f)(1)(ii). Importantly, certain big-dollar donations are excluded from this calculation, requiring charities to seek out a variety of donors rather than rely on a few high-net-worth supporters. *See id.* § 1.170A-9(f)(3)(iii)(B). In other words, IRS regulations effectively force charitable and educational organizations to collect massive amounts of consumer data to survive. *See* I.R.C. § 170(b)(1)(A)(vi) (defining category of 501(c)(3) organizations subject to public support requirements); 26 C.F.R. § 1.170A-9(f)(1)-(3) (detailing one-third public support calculation and limitations on big-dollar donations); *see also* Ely R. Levy & Normal I. Silber, *Nonprofit Fundraising and Consumer Protection: A Donor's Right to Privacy*, 15 STAN. L. & POL'Y REV. 519, 528-29 (2004) (stating "almost all" nonprofit donations, subscriptions, communications, and service requests "leave behind ... [an] electronic record," making the nonprofit sector's data presence "no less sophisticated and complex than the commercial one").

32. *See* Levy & Silber, *supra* note 31, at 528.

33. *See id.* at 528, 535.

broad categories that implicate assistance to, and programs for, individuals.[34]

Because exempt charitable organizations are forced to seek a diverse donor base by virtue of Internal Revenue Service regulations and are similarly confined to a narrow set of permissible purposes in their operations, the nature of the 501(c)(3) exemption is one that demands a continuous intake and use of consumer data.[35]

II. COMPLEXITY OF EXISTING PATCHWORK SYSTEM

The landscape of consumer data privacy measures is dominated by individual jurisdictions' attempts at drafting and instituting consumer-protective schemes that sweep beyond the jurisdictions' own borders.[36] Each consumer data privacy law[37] defines personal data and covered entities differently and provides for a wide range of enforcement actions in the event of a compliance shortcoming or failure.[38]

---

34. *See* I.R.C. § 501(c)(3) (defining exempt purposes for which an entity must be organized and operated to be granted federal tax exemption under the section). Note that the IRS describes "charitable" as including relief to "the poor, the distressed, or the underprivileged," the elimination of "prejudice and discrimination," and the defense of "human and civil rights." *Exempt Purposes—Internal Revenue Code Section 501(c)(3)*, IRS (Sept. 7, 2021), https://www.irs.gov/charities-non-profits/charitable-organizations/exempt-purposes-internal-revenue-code-section-501c3 [https://perma.cc/8BEN-B4YX]. The people-centric nature of these permissible purposes is evident.

35. *See supra* notes 29-33 and accompanying text.

36. *See, e.g.*, GDPR, *supra* note 10, at art. 3(1)-(3) (establishing that the measure "applies to the processing of personal data ... regardless of whether the processing takes place in the [European] Union or not").

37. This Note only considers enacted, comprehensive consumer data privacy measures in existence as of February 2022, which does not include the since-enacted Utah Consumer Privacy Act (signed into law March 24, 2022) or Connecticut's Act Concerning Personal Data Privacy and Online Monitoring (signed into law May 10, 2022). *See* 2022 Utah Laws 462 (effective Dec. 31, 2023); 2022 Conn. Acts 22-15 (Reg. Sess.) (effective July 1, 2023). While numerous category-specific data privacy measures exist beyond the European scheme and three state-level comprehensive measures highlighted here, these laws are often focused on one subset of consumer data and are not as relevant to 501(c)(3) groups. *See, e.g.*, Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1-14/99 (2008).

38. *Compare, e.g.*, GDPR, *supra* note 10, at art. 4(1) (defining "personal data" to mean "any information relating to an ... identifiable natural person"), *with, e.g.*, CAL. CIV. CODE § 1798.140(o)(1) (West 2023) (defining "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer").

To illustrate the difficulty of good-faith compliance with all applicable measures, this Section compares four key elements of each existing comprehensive consumer data privacy measure: the definition of personal data or information, the scope of applicability relative to 501(c)(3) organizations, what full compliance with the measure demands, and the enforcement mechanisms and consequences provided for compliance failures.

A. Existing Comprehensive Consumer Privacy Measures

Four major consumer data privacy laws have implications for 501(c)(3) organizations: the European Union's General Data Protection Regulation, California's Consumer Privacy Act, Colorado's Privacy Act, and Virginia's Consumer Data Privacy Act.[39] While the 117th Congress has introduced a sweeping federal measure, the Consumer Data Privacy and Security Act of 2021, that would preempt state law in this area, the bill has failed to gain traction in either chamber.[40]

1. European Union General Data Protection Regulation

The GDPR was adopted in April 2016[41] and went into effect in May 2018.[42] The GDPR defines personal data incredibly broadly as "any information relating to an identified *or* identifiable natural person."[43] This definition is understood to include not only biographical information about natural persons, such as names, addresses, and birthdates, but also data such as "log-in information, IP

39. *See supra* notes 8 and 10. Again, this discussion exempts the Utah Consumer Privacy Act and Connecticut's Act Concerning Personal Data Privacy and Online Monitoring, which were enacted after this Note's writing. *See supra* note 37.

40. Consumer Data Privacy and Security Act of 2021 (CDPSA), S. 1494, 117th Cong. (2021). Notably, § 2(4)(A)(ii)(III) of the draft bill explicitly *includes* nonprofit organizations as entities required to comply with the proposal. S. 1494 § 2(4)(A)(ii)(III). Thus, the bill takes the opposite position of the one taken by this Note.

41. *The History of the General Data Protection Regulation*, EUR. DATA PROT. SUPERVISOR (2022), https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [https://perma.cc/GSW5-6E43].

42. Directorate-General for Communication, *Data Protection in the EU*, EUR. COMM'N (2021), https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [https://perma.cc/KT7Y-N9AP].

43. GDPR, *supra* note 10, at art. 4(1) (emphasis added).

addresses, and vehicle identification numbers," because these details enable indirect identification of natural persons.[44]

The GDPR applies to organizations involved in controlling or processing the personal data of individuals located within the European Union, with "processing" broadly defined to capture any operation performed on personal data (either individually or in sets).[45] Crucially, these definitions are explicitly expanded by specific territorial provisions outlined in Article 3 of the GDPR.[46] Article 3 establishes that the regulation applies to all processing of personal data of "subjects who are in the [European] Union" by an entity *not* in the European Union when the data processing activities are related to the offering of goods or services to individuals in the EU, even if the goods or services are offered free of charge (such as those of a tax-exempt organization).[47]

For a 501(c)(3) organization, then, determining if the organization's web presence, online programming, or other operations constitute the "offering" of goods and services to a European Union member state is critically important.[48] The GDPR makes clear that mere website access within the Union is insufficient to demonstrate that an entity is actively offering goods and services to EU data subjects, but beyond this bright line, the measure is murky.[49] The GDPR suggests a multifactor assessment to determine if an organization is indeed offering goods or services to the European Union, which considers, among other elements, the organization's use of the language or currency of a member state and if the organization mentions EU customers.[50]

---

44. Caroline Krass, Alexander H. Southwell, Ahmed Baladi, Emanuelle Bartoli, James A. Cox, Michael Walther, Ryan T. Bergsieker & Jason N. Kleinwaks, *The General Data Protection Regulation: A Primer for U.S.-Based Organizations That Handle EU Personal Data*, GIBSON DUNN (Dec. 4, 2017), https://www.gibsondunn.com/the-general-data-protection-regulation-a-primer-for-u-s-based-organizations-that-handle-eu-personal-data/ [https://perma.cc/Z7KP-XCH5] (noting that, due to definitional breadth, "in practice, most services and/or projects will be considered to involve processing of personal data").

45. GDPR, *supra* note 10, at art. 4(2).

46. *Id.* at art. 3(1)-(3).

47. *Id.* at art. 3(2)(a).

48. *See id.* at reg. (23).

49. *See id.*

50. *Id.*

The GDPR's compliance requirements are extensive and largely depend on whether a covered actor is classified as a "controller" of personal data, a "processor" of personal data, or both.[51] Covered organizations that are determined to "offer goods or services" to the Union "must designate [an official] representative to the European Union in writing."[52] Additional duties of "controllers," defined as businesses that determine the means and purposes of personal data processing, include lengthy transparency requirements and a responsibility to ensure the legality of every stage of the data processing scheme.[53] In practice, this controller liability "can only be achieved by way of complete documentation" that is quite burdensome to covered entities.[54] Controllers must also meet breach notification standards and conduct periodic data protection impact assessments depending on the nature of the data-related activity at hand.[55]

Member states of the European Union are granted broad enforcement powers under the GDPR, including investigative rights and the ability to impose administrative fines for infringements.[56] These fines can be substantial, with a maximum penalty of €20 million or 4 percent of an offender's annual revenue, whichever is higher.[57] European regulators have not been shy about enforcement, issuing fines as large as €50 million over the first four years the measure has been in effect.[58] Given the average budgets of 501(c)(3)

---

51. *See* Manuel Klar, *Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies*, 11 HASTINGS SCI. & TECH. L.J. 101, 141-43 (2020). The breadth of the GDPR's compliance obligations is also a product of the breadth of the consumer rights granted under the measure. *See* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 365 (2019) (summarizing key GDPR-granted consumer rights as a right to access data, a right to portability, a right to be forgotten, and a right to know if data has been hacked).

52. *See* Klar, *supra* note 51, at 142.

53. *See id.* at 144-46.

54. *Id.* at 150-53.

55. *Id.* at 151-53.

56. GDPR, *supra* note 10, at arts. 58, 83.

57. *See id.* at art. 83(4)-(5).

58. *See Three Years of GDPR: The Biggest Fines So Far*, BBC (May 24, 2021), https://www.bbc.com/news/technology-57011639 [https://perma.cc/4CQX-ECXD] (describing significant fines issued over first three years of GDPR operation).

organizations, it is obvious that a fine of this size would drive an organization out of business.[59]

In short, the GDPR is deliberately designed to capture a huge range of for- and nonprofit entities that process the personal data of those within the European Union and carries a hefty deterrence element in the form of threatened multi-million-euro penalties.[60] As most tax-exempt organizations could be classified as their own "controllers" of data (assuming the preconditions of offering goods or services to EU member states are met), compliance with the GDPR represents a huge and potentially ruinous barrier to Small-town Charity-*esque* organizations.[61]

2. California Consumer Privacy Act

The California Consumer Privacy Act, passed in June 2018 and effective January 2020, was the United States' first exposure to a domestic, GDPR-style, comprehensive privacy measure.[62] Almost immediately, the CCPA earned comparisons to the GDPR and was regarded as the most sweeping privacy law in the United States.[63] Given the oversized reach of California's economy—both relative to the rest of the United States and to the remainder of the globe—the CCPA attracted immediate attention as a privacy measure in a

---

59. *See supra* note 11 and accompanying text.

60. *See supra* notes 41-57 and accompanying text.

61. *See supra* Introduction. Note that this discussion of the GDPR is provided solely as background for the American variations on the European approach to comprehensive privacy measures. This Note is not focused on detailing American charities' compliance under the GDPR.

62. *See* Joshua A. Jessen, Benjamin B. Wagner, Christina Chandler Kogan, Abbey A. Barrera & Alison Watkins, *California Consumer Privacy Act of 2018*, GIBSON DUNN (July 12, 2018), https://www.gibsondunn.com/california-consumer-privacy-act-of-2018/ [https://perma.cc/326A-L5BF]. Note that the CCPA has already been amended multiple times since its enactment, mostly for technical adjustments and the extension of regulatory-related deadlines. *See generally CCPA-/CPRA-Related Legislation Tracker*, INT'L ASS'N PRIV. PROS. (Feb. 27, 2022), https://iapp.org/resources/article/ccpa-cpra-related-legislation-tracker/ [https://perma.cc/7H54-BT6W] (cataloging ongoing amendments to the CCPA).

63. *See, e.g.*, Jessen et al., *supra* note 62 (introducing the CCPA as being "not as strict as the EU's new General Data Protection Regulation (GDPR)," but still "more stringent than most privacy laws in the United States").

jurisdiction in which American entities were very likely to be active.[64]

Like the GDPR, the CCPA's definition of personal data (termed "personal information" in the statute) is exceptionally broad. The Act describes personal information as information that not only directly identifies a particular consumer, but also as information that "relates to, describes, [or] is reasonably capable of being associated with" a specific individual, even if indirectly.[65] Among other categories of covered data, the CCPA notes that names, physical addresses, online usernames, email addresses, internet browsing history, professional or employment history, and "[i]nferences drawn from any of the information identified ... to create a profile about a ... consumer's preferences" are all definitively considered personal information.[66]

The CCPA applies to businesses that meet specific data processing or revenue-based thresholds outlined in the text.[67] Because the California Act defines "business" to mean entities that are organized or operated for profit, 501(c)(3) organizations are generally not required to comply with the CCPA's prescriptions.[68] However, entities that are controlled by for-profit businesses or that share corporate branding may be captured under the CCPA.[69] With the rise in corporate foundations and fundraising mechanisms such as commercial co-venture campaigns, the CCPA could capture California-operating 501(c)(3) organizations that have close relationships with a controlling for-profit entity.[70]

---

64. *See Best States for Business 2019, California*, FORBES (2019), https://www.forbes.com/places/ca/ [https://perma.cc/W2D9-3MVW] (noting California's economy represents 15 percent of the United States' and would rank as the fifth biggest in the world if it were an independent country).

65. CAL. CIV. CODE § 1798.140(o)(1) (West 2023).

66. *Id.* § 1798.140(o)(1)(A)-(K).

67. *Id.* § 1798.140(c)(1)-(2).

68. *See id.*

69. *Id.* § 1798.140(c)(2) (defining business to also include "[a]ny entity that controls or is controlled by a business ... and that shares common branding with the business").

70. *Id.* For a description of commercial co-ventures, sometimes termed "cause marketing," see *Commercial Co-Ventures and Cause Marketing*, HARBOR COMPLIANCE (May 18, 2022), https://www.harborcompliance.com/information/commercial-co-ventures-and-cause-marketing [https://perma.cc/5QBV-ACBM]; *see also Commercial Co-Ventures and Cause-Related Marketing*, NAT'L COUNCIL OF NONPROFITS, https://www.councilofnonprofits.org/tools-resources/commercial-co-ventures-and-cause-related-marketing [https://perma.cc/Z744-M3ZW].

California's Act centers on providing consumers with rights related to how and why their personal data is used.[71] As indicated in the original draft legislation, the goal of the CCPA is to ensure Californians' rights to (1) know what data is collected and stored by businesses, (2) learn whether their personal data is sold or shared, (3) refuse the sale of personal information to third parties, and (4) access and control their personal data, including a right to delete said data upon request.[72] The obligations imposed on covered businesses mirror these consumer-oriented aims.[73] Among other responsibilities, CCPA-compliant businesses must utilize elaborate data-tracking software systems to respond to consumer requests about the specifics of the personal data a business may hold about the consumer.[74] Covered entities are also required to provide multiple mediums through which a consumer may contact the business to request their personal information, and businesses must also institute transparency practices at the point of data collection and in response to consumer requests for data deletion.[75]

While the compliance efforts described above may only require minor adjustments from well-resourced and technology-savvy for-profit organizations, such systems are a far cry from the record-keeping systems that are used in good faith by the Smalltown Charities of the world were they to be "captured" by the CCPA's narrow coverage of (c)(3)-exempt groups.[76] The majority of the CCPA's provisions are to be enforced by the Attorney General of California, who is empowered to seek civil penalties up to $2,500 per violation of the Act.[77] Higher penalties may be sought for intentional violations.[78] Consumers are granted a private right of action only in response to data breaches, in which case plaintiffs may recover up to $750 per infraction, or actual damages, whichever is greater.[79]

---

71. *See* CAL. CIV. CODE § 1798.100. Significantly, the first section of the statute opens with a statement of consumer rights granted therein. *Id.* § 1798.100(a).

72. Assemb. Bill 375, 2017-2018 Reg. Sess., Ch. 55, Sec. 2(i) (Cal. 2018).

73. *See generally* Jessen et al., *supra* note 62 (outlining compliance requirements under CCPA).

74. CAL. CIV. CODE § 1798.110(b)-(c).

75. *Id.* §§ 1798.100, .110.

76. *See supra* notes 6-11 and accompanying text.

77. CAL. CIV. CODE § 1798.155(b).

78. *Id.*

79. *Id.* § 1798.150(a)-(b).

If the CCPA is California's response to the GDPR, it sounds more like an echo than an answer.[80] The two measures track very closely in their scope, reaching beyond the European Union and California alike to pull foreign entities into the compliance web—and at a cost when compliance falls short.[81]

3. Virginia Consumer Data Protection Act

Virginia became the second state to join the consumer data privacy patchwork regime, enacting the Virginia Consumer Data Protection Act in March 2021 and adding an East Coast flair to an American legislative arena previously dominated by the Golden State.[82] Though some of the Virginia measure's language is familiar to readers of the CCPA, the VCDPA makes meaningful departures from California's system and embraces a European-style policy with a specific exemption for 501(c)(3) organizations.[83]

Virginia's law defines "personal data" broadly: any information that is linked or reasonably connectable to an identified natural person (or *identifiable* individual) is considered personal data, with exemptions for publicly available information and employment-related details.[84] "Sensitive" data "revealing" a consumer's racial, ethnic, religious, health, and/or sexual identities is granted additional protection.[85]

Unlike the California model (but similar to Colorado's measure discussed in Part II.A.4 of this Note), Virginia's law does not set a revenue threshold to determine the statute's applicability.[86] Rather, the Act applies based on an entity's contacts with Virginia resident-

80. *See supra* Part II.A.1-2.

81. *See supra* Part II.A.1-2.

82. *See* VA. CODE ANN. § 59.1-575 (2021); Alexander H. Southwell, Ryan T. Bergsieker, Cassandra L. Gaedt-Sheckter, Frances A. Waldmann & Lisa V. Zivkovic, *Virginia Passes Comprehensive Privacy Law*, GIBSON DUNN (Mar. 8, 2021), https://www.gibsondunn.com/virginia-passes-comprehensive-privacy-law/ [https://perma.cc/WK45-CV42].

83. *Compare supra* Part II.A.2 (summarizing California policy), *with supra* Part II.A.1, *and infra* Part II.A.3 (discussing European Union GDPR and Virginia's privacy measure, respectively).

84. VA. CODE ANN. § 59.1-575. Information made available to the public via the media is considered publicly available information not covered by the Act. *Id.*

85. *Id.* §§ 59.1-575, -580.

86. *Compare supra* Part II.A.2 (noting California revenue-based applicability thresholds), *with infra* Part II.A.4 (discussing Colorado's lack of monetary threshold).

consumers, regardless of revenue generated in the Commonwealth or from processing personal data.[87] To be regulated under the VCDPA, entities must (1) conduct business in Virginia or target goods or services to residents of the state and (2) control or process the personal data of at least one hundred thousand Virginians during a given calendar year.[88] Notably, neither "conduct business" nor "target residents" is defined in the law.[89]

Significantly, however—and at the heart of this Note—is Virginia's explicit exemption of nonprofit organizations. The VCDPA carves out "nonprofit organization[s]" from compliance, which the statute defines as "any corporation organized under the Virginia Nonstock Corporation Act or any organization exempt from taxation under § 501(c)(3) ... of the Internal Revenue Code."[90] In other words, the Act exempts exactly the type of organization formed by the Smalltowners in this Note's introduction: both Virginia-formed nonprofit organizations and 501(c)(3)-exempt groups are excused from complying with the VCDPA's demands.[91]

The VCDPA grants Virginia consumers access, correction, deletion, portability, antidiscrimination, opt-out, and business appeal rights.[92] As with the regimes reviewed in Parts II.A.1 and II.A.2, businesses' obligations under the VCDPA mirror consumer rights granted: covered organizations must implement extensive data security practices (including administrative, physical, and technical safeguards), provide conspicuous means by which consumers may exercise their data rights, and obtain consent for certain uses of data outside the scope of uses previously disclosed to Virginians.[93] Perhaps the most costly obligation from the GDPR, the

87. VA. CODE ANN. § 59.1-576(A).

88. *Id.* Note that the VCDPA, similar to the CPA, has a second applicability definition that requires compliance from entities that both process or control the data of twenty-five thousand Virginians per calendar year and receive at least 50 percent of their gross revenue from the sale of personal data. *Id.* As this definition is unlikely to capture 501(c)(3) charitable organizations, it is not discussed as a comparative point between statutory regimes.

89. *See id.* § 59.1-575 (failing to include conduct of business or targeting of residents in definitional section of enacted bill).

90. *Id.* §§ 59.1-575, -576(B) (citation omitted). Organizations exempt under §§ 501(c)(6) and 501(c)(12)—trade associations and mutual insurance entities—are also carved out of the VCDPA. *See id.* If only the Smalltowners had read the definition recital more carefully!

91. *See id.*

92. *Id.* § 59.1-577(A), (C).

93. *Id.* § 59.1-578(A)(2)-(3), (C).

conduct of periodic data protection assessments, is also incorporated into the VCDPA—though the Act does not specify how often these evaluations must be conducted.[94]

Enforcement of the VCDPA is delegated to the Virginia Attorney General, who is empowered to seek injunctions and damages up to $7,500 per infraction.[95] In contrast with California's provisions, no private right of action is granted to consumers under Virginia's Act.[96] This suggests the measure's efficacy could be subject to the Commonwealth's political swings because the Virginia Attorney General is an elected official with a four-year term.[97] The VCDPA was passed through a Democrat-controlled Virginia General Assembly and with a Democrat Attorney General in office—a political reality recently changed with January 2022's inauguration of a new Republican Governor and Attorney General.[98]

Virginia's Act therefore succeeds in bringing to life the heart of this Note's argument: that a comprehensive consumer data privacy measure should provide an exemption for section 501(c)(3)-exempt charitable and educational organizations.[99] Without this explicit exemption, it is plain that the demands of the VCDPA would otherwise be fatal to the Smalltown Charities of the Commonwealth (at least during administrations that aim to enforce the Act).[100]

4. Colorado Privacy Act

With its July 2021 passage of the Colorado Privacy Act, the Centennial State joined California and Virginia as the third to protect

94. *See id.* § 59.1-580(A). Data processing assessments are required only for certain enumerated processing purposes, such as the use of personal data in targeted advertising. *Id.* § 59.1-580(A)(1).

95. *Id.* § 59.1-584(A), (C).

96. *Compare id.* (providing only for Attorney General-led enforcement action), *with* CAL. CIV. CODE § 1798.150(a)-(b) (West 2023) (providing private right of action).

97. *See* VA. CONST. art. 5, § 15 (providing for election of the Attorney General).

98. *See* Matthew Barakat, *Miyares Elected Virginia Attorney General, Denying Herring a 3rd Term*, PBS NEWSHOUR (Nov. 3, 2021), https://www.pbs.org/newshour/politics/miyares-elected-virginia-ag-denies-herring-3rd-term [https://perma.cc/EFF5-A3N2]. Republican Attorneys General may be just as eager to enforce the measure as their Democratic counterparts; this footnote only highlights the potentially fluid enforcement landscape as the Office of the Attorney General changes political hands.

99. *See infra* Part III; VA. CODE ANN. § 59.1-576(B).

100. *See supra* Part II.A.3 (describing compliance obligations under Act).

individual privacy rights with GDPR-style legislation.[101] While the Colorado measure parallels its Californian and Virginian predecessors in certain regards, the CPA does not exempt any category of nonprofit organizations and adopts specific European-style ongoing compliance obligations as part of its framework.[102]

In language that echoes the measures previously discussed in this Note, the CPA defines personal data as information "linked or reasonably linkable to an identified or identifiable individual."[103] The Act explicitly excludes publicly available information from this definition, permitting entities to process or control data without CPA applicability if the data is either made available by governmental authorities or is reasonably believed to be made available to the general public by the consumer.[104] A subdefinition of "sensitive data" controls for the Act's consent requirements, covering information that "reveal[s] racial or ethnic origin, religious beliefs, a mental or physical health condition[,] ... sexual orientation, or citizenship" and data collected about a "known child."[105]

The CPA differs from its coastal counterparts in its inclusion of nonprofit organizations in its compliance net.[106] Generally, the Act applies to any entity that (1) conducts business in Colorado or offers services that are targeted to Coloradoans, and (2) meets a defined, quantitative data processing threshold.[107] The CPA does not set a revenue floor for compliance; rather, the measure applies to organizations that either control or process the personal data of one hundred thousand or more Coloradoans during a calendar year,

---

101. *See* Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected Under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA HIGH TECH. L.J. 39, 73 (2021).

102. *See* COLO. REV. STAT. § 6-1-1304(1) (effective July 1, 2023) (defining applicability of statute independent of entity's non- or for-profit status); Buresh, *supra* note 101, at 73-74.

103. COLO. REV. STAT. § 6-1-1303(17)(a).

104. *Id.* § 6-1-1303(17)(b).

105. *Id.* §§ 6-1-1303(24), -1308(7).

106. *Compare supra* Part II.A.2-3 (discussing CCPA and VCDPA nonprofit exemptions), *with* COLO. REV. STAT. § 6-1-1304(1) (defining applicability of statute).

107. COLO. REV. STAT. § 6-1-1304(1). Note that the statute does not define what constitutes "conducting business," nor does the Act clarify what "targeted services" entails. *See id.* § 6-1-1303.

regardless of income derived from that controlling or processing.[108] In plain language, the CPA likely captures organizations that continuously interact with Coloradoans, including nonprofit entities that may be exempted from other states' privacy regimes.[109]

Consumers are granted six (rather familiar) rights under the CPA: the right of access, the right to correct inaccuracies, the right to deletion, the right of portability, the right to opt-out, and the right to appeal.[110] To effectuate these rights, the CPA requires covered organizations to adopt security measures for confidentiality, conduct periodic GDPR-style data protection assessments, collect only personal data "reasonably necessary" to a disclosed business purpose, and establish opt-in and opt-out procedures for consumers to vindicate their consent rights.[111]

While consumers are not granted a private cause of action to enforce the CPA, the state's Attorney General and district attorneys are empowered to bring suit against noncompliant organizations that fail to remedy violations within sixty days of notification.[112] Though the Act itself does not provide for penalties, violation of it is considered a deceptive trade practice under Colorado law.[113] Each violation may be subject to a penalty of up to $20,000, with the Attorney General and district attorneys being granted substantial discretion for setting fines.[114]

Of the three state measures examined in Part II of this Note, the CPA imposes the highest compliance obligation on 501(c)(3)

---

108. *Id.* § 6-1-1304(1). Note that the statute has a second applicability definition that requires compliance from entities that both process or control the data of twenty-five thousand Colorado residents per calendar year and receive revenue from the sale of personal data. *Id.* § 6-1-1304(1)(b)(II). Because this second definition is highly unlikely to capture 501(c)(3) charitable organizations, it is not discussed as a comparative point between statutory regimes.

109. *See* Ryan Bergsieker, Sarah Erickson, Lisa Zivkovic & Eric Hornbeck, *The Colorado Privacy Act: Enactment of Comprehensive U.S. State Consumer Privacy Laws Continues*, GIBSON DUNN (July 9, 2021), https://www.gibsondunn.com/the-colorado-privacy-act-enactment-of-comprehensive-u-s-state-consumer-privacy-laws-continues/ [https://perma.cc/9KUE-JR5L].

110. Buresh, *supra* note 101, at 73-74.

111. Bergsieker et al., *supra* note 109; Buresh, *supra* note 101, at 74.

112. COLO. REV. STAT. § 6-1-1311(1).

113. *Id.* § 6-1-1311(1)(c).

114. *Id.* § 6-1-112(1)(a). Note that a violation of any part of the CPA is considered a separate violation per consumer. *Id.*

organizations by failing to exempt any not-for-profit entities.[115] Though the Rocky Mountain economy may not match California's mammoth scale, charitable organizations with Coloradoan connections may nonetheless be required to overhaul their internal systems due to the CPA's unique, revenue-independent applicability definition.[116]

B. Federal Preemption Attempts

While states are currently the only American jurisdictions coloring the privacy patchwork, consumer data issues are not far from the federal government's mind.[117] Most importantly for this Note, pending before the 117th Congress is a comprehensive, preemptory consumer data privacy measure that would explicitly *include* nonprofit organizations in its compliance web.[118] Though the political reality of the 117th Congress points to a bleak outlook on the measure's likelihood of passage (if only due to Washington's incessant partisan gridlock), the federal bill is nonetheless informative in providing an example of express preemption of state law in the consumer data privacy arena.[119]

The draft CDPSA uses a familiar definition for personal data and applies broadly to all entities over which the Federal Trade Commission has oversight authority.[120] The bill explicitly includes nonprofit organizations in its coverage, noting that the measure would empower the Federal Trade Commission to "enforce this Act, with respect to ... nonprofit organizations ... in the same manner

---

115. *See supra* notes 101-14 and accompanying text.

116. *See* COLO. REV. STAT. § 6-1-1304(1)(a).

117. *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1777 (2021) (counting at least ten federal data privacy proposals that were introduced in 2018 and 2019). *But see supra* note 37 (acknowledging the newly-enacted Utah and Connecticut comprehensive privacy measures but restricting this Note to the measures in effect at the time of writing in February 2022).

118. Consumer Data Privacy and Security Act of 2021 (CDPSA), S. 1494, 117th Cong. § 2(4)(A)(ii)(III) (including "nonprofit organization[s]" as covered entities under the measure).

119. *Id.* § 10(a)-(b) (providing for "express preemption of state law").

120. *Id.* §§ 2(4)(A), 9(2)(A)-(C) (defining covered entity as any entity over which the Federal Trade Commission has authority, which generally includes all businesses except financial institutions and air carriers, and further defining personal data as information that identifies, is linked, or is easily linkable to a specific individual).

provided" for enforcement against for-profit organizations.[121] "Nonprofit organization" is not separately defined in the draft measure, though would likely include 501(c)(3) organizations under a reasonable reading of the term.[122]

In general, the draft CDPSA inflicts fewer compliance requirements on covered entities than existing state-level measures. The bill provides consumers with knowledge, access, and erasure rights, which would require covered businesses to (1) institute clearly worded and comprehensive privacy policies, (2) develop ongoing notification systems for policy changes, (3) create portability and erasure mechanisms, and (4) obtain affirmative consent for most personal data uses.[123] The Federal Trade Commission would be tasked with enforcement of the measure, though state attorneys general would also be granted a cause of action in federal court for violations that uniquely harm their respective states.[124] No private cause of action would exist under the bill as currently drafted.[125]

Crucially, the CDPSA would provide a singular blanket to replace the (arguably ineffective, noncomprehensive, and troublesome) existing patchwork: the bill remarks that it is the "express intention of Congress to promote consistency ... through the establishment of a uniform Federal privacy framework that preempts ... the authority of any State or political subdivision of a State."[126] Thus, the pending Federal Act of 2021 would address the fragmentary nature of existing state-level privacy legislation, but would not remove 501(c)(3) organizations from its coverage.[127]

---

121. *Id.* § 9(a)(2)(C).

122. *See Nonprofit Corporation*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("A corporation organized for some purpose other than making a profit, and usu[ally] afforded special tax treatment.").

123. S. 1494, §§ 3(a)(1), 4(a), 5(b)-(d).

124. *Id.* § 9(a)-(b).

125. *Id.* § 9(d).

126. *Id.* § 10(a).

127. *See supra* notes 117-26 and accompanying text.

III. A CASE FOR FEDERAL PREEMPTORY ACTION THAT EXEMPTS 501(C)(3)S

There exists little doubt that the federal government—or at least Congress—understands the need to pass a comprehensive consumer data privacy measure that preempts state law.[128] How, then, should such a hypothetical privacy measure take shape?

This Part first examines Congress's Commerce Clause power under current Supreme Court interpretation to establish that a comprehensive, preemptory consumer data privacy measure is within the federal legislature's power to enact—with or without an explicit 501(c)(3) organization exemption.[129] After establishing the constitutional groundwork, this Part will focus on normative arguments for an omnibus bill, emphasizing (1) the public policy interest in the continued existence of 501(c)(3) organizations, (2) the lower potential of abuse of the exemption by 501(c)(3) groups by virtue of their Internal Revenue Service-imposed expenditure limitations, and (3) the need to properly balance the individual privacy right against a market-wide interest in avoiding mass nonprofit organization bankruptcy.[130]

A. Commerce Clause Power Permits Congressional Action

Despite the Commerce Clause's steady growth into the most expansive of Congress's granted and enumerated powers, outlining a constitutional argument for the ability of the federal government to institute an omnibus consumer data privacy measure is crucial for legitimizing the hypothetical legislation.

Under current interpretation of the Commerce Clause power, Congress receives substantial deference in determining that a

---

128. *See* Chander et al., *supra* note 117, at 1777 (noting at least ten omnibus federal measures in this area have been introduced in 2018-2019 alone).

129. While some academics have simply assumed the Commerce Clause to cover this sort of legislation, outlining a baseline Commerce Clause argument is necessary to ground the rest of the discussion. *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 922 (2009) (explicitly assuming a federal privacy "omnibus law" is "constitutionally permissible" given the "scope of the Commerce Clause").

130. *See infra* Part III.B.

regulated area impacts interstate commerce.[131] While recent case law surrounding healthcare measures has somewhat complicated the Commerce Clause inquiry, the Supreme Court has interpreted the Clause to grant Congress the power to regulate (1) the use of channels of interstate commerce (such as railroads), (2) instrumentalities of interstate commerce (such as individual persons), and (3) local activities that substantially impact interstate commerce.[132] Economic "local activities" receive substantial deference: so long as there is a rational connection between the activity being regulated and interstate commerce, the Court's inquiry ends and the measure is upheld.[133]

In the realm of consumer data privacy, Congress has already drawn explicit connections between its Commerce Clause power and prior privacy legislation, legislation that has not been reworked or overruled by the Court.[134] While it therefore seems unlikely that a comprehensive federal consumer data privacy measure would be challenged for exceeding the scope of Congress's Commerce Clause power (given the public and the Court's amenability to congressional activity in this area thus far), such a measure would squarely fit into the Clause's test outlined above.[135]

First, there is a colorable argument that the internet is now both a "channel" and an "instrumentality" of interstate commerce, giving Congress the ability to regulate transactions that occur online in the same manner as regulating a railroad or persons moving across

131. U.S. CONST. art. 1, § 8, cl. 3; *see, e.g.*, Gonzales v. Raich, 545 U.S. 1, 22 (2005) (articulating a "rational basis" standard for review of congressional interstate commerce regulation).

132. United States v. Lopez, 514 U.S. 549, 558-59 (1995) (defining these three "broad categories of activity that Congress may regulate under its commerce power").

133. *Compare, e.g.*, Heart of Atlanta Motel v. United States, 379 U.S. 241, 255-56, 261-62 (1964) (holding that movement of travelers between states is commercial, economic activity regulatable by Congress under the Clause and upholding antidiscriminatory public accommodation provisions of Title VII of the Civil Rights Act of 1964 as a result), *with, e.g.*, United States v. Morrison, 529 U.S. 598, 613-14, 627 (2000) (holding that gender-motivated violent crimes are not economic activity and striking down portion of Violence Against Women Act as a result).

134. *See* Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 878-79 n.36 (2009) (providing examples of legislation in which Congress has connected its interstate commerce regulatory capability to consumer privacy; for example, the definition of "wire communication" in 18 U.S.C. § 2510(1)).

135. *See supra* notes 131-34 and accompanying text.

state lines.[136] This characterization of the internet would permit congressional regulation of consumer data privacy without additional review of Congress's rationale.[137]

Yet even without classifying the internet as a channel or instrumentality of commerce, Congress indubitably has a rational basis for concluding that consumer data privacy activity impacts the interstate marketplace, especially if taken in the aggregate.[138] The nonprofit organization activities implicated by the hypothetical data privacy measure—soliciting and processing donations, conducting targeted activity in their communities, and utilizing contributor data for future marketing—are illustrative of the economic heart of a consumer data privacy measure.[139] Congress could undoubtedly conclude (and, arguably, already has concluded) that such data processing and controlling activities, occurring on a borderless platform like the internet, impact interstate commerce to a degree that justifies federal preemptory action.[140]

In short, the case for Congress's ability to pass a comprehensive consumer data privacy measure that replaces and preempts state and local law is effectively airtight. The Constitution's constraints should not be considered a barrier to congressional action in this policy area.[141]

B. Scope of Measure Would Ensure Constitutionality

Despite the imagined measure's relatively uncontroversial constitutional basis, the Supreme Court's recent history of Affordable Care Act (ACA) litigation illustrates a potential retreat from

---

136. *See, e.g.*, United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) ("As both the means to engage in commerce and the method by which transactions occur, 'the Internet is an instrumentality *and* channel of interstate commerce.'") (internal citation omitted) (emphasis added)).

137. *See id.* ("No additional interstate nexus is required when instrumentalities or channels of interstate commerce are regulated.").

138. *See, e.g.*, Wickard v. Fillburn, 317 U.S. 111, 127-28 (1942) (permitting the aggregation of individual contributions to interstate commerce in which the collective impact is "far from trivial").

139. *See generally supra* Parts I and II.

140. *See supra* note 134 and accompanying text.

141. *See supra* Part III.A.

expansive interpretations of the Commerce Clause.[142] Of concern to the ideal consumer data privacy preemptory measure exempting 501(c)(3) organizations is the scepter wielded by the Supreme Court's Commerce Clause analysis in *National Federation of Independent Businesses v. Sebelius*.[143] Chief Justice Roberts's majority held that the ACA's individual mandate did not regulate existing commercial activity but rather "compel[led] individuals to *become* active in commerce" through the purchase of health insurance.[144] In short, the Chief Justice's opinion held that what is inherently noneconomic, and non-regulatable, cannot become economic and regulatable merely by the stroke of Congress's pen.[145]

This argument was forceful enough for the Court to look to Congress's taxing power to uphold the Act.[146] With the now-expanded conservative majority on the Court, it is not unreasonable to anticipate heightened scrutiny of novel uses of congressional Commerce Clause power.[147] To survive Supreme Court review, then, the hypothesized preemptive consumer data privacy measure must take care to avoid regulating what the Supreme Court could interpret as being noninterstate *or* noneconomic for the purposes of the Commerce Clause.

Carefully defining the applicability of the measure should avoid the risk of the legislation being found to cover noninterstate activity outside the scope of the Clause. The answer lies in precise drafting: the federal preemptory measure contemplated by this Note must apply only to organizations that engage in truly interstate consumer data activities—a connection that Congress must be explicit in

142. *See* Nat'l Fed'n of Indep. Bus. v. Sebelius, 567 U.S. 519, 588 (2012) (holding Affordable Care Act's individual mandate impermissible under congressional Commerce Clause power but constitutional under Congress's taxing power).

143. *Id.* at 552 (reasoning that the individual mandate, which required individuals to purchase health insurance, was not a regulation of existing economic activity nor interstate in nature).

144. *Id.*

145. *See id.*

146. *Id.* at 561-66.

147. *Id.* at 563 (upholding the mandate as an imposition of a tax under Congress's taxing power); *see also* Jody Freeman, *What Amy Coney Barrett's Confirmation Will Mean for Joe Biden's Climate Plan*, VOX (Oct. 26, 2020, 10:18 AM), https://www.vox.com/energy-and-environment/ 21526207/amy-coney-barrett-senate-vote-environmental-law-biden-climate-plan [https://perma.cc/3ERM-MUVY] (discussing Justice Barrett's past praise of the Court's Commerce Clause analysis in ACA litigation).

drawing legislatively. Purely local organizations should be excluded from the measure's coverage entirely, even if those organizations' operations could theoretically fall under the *Lopez* exception for local activities.[148] Crucially, the exemption of 501(c)(3) organizations from compliance with the federal legislation should similarly cover only charitable entities whose data activities are properly understood as "interstate."[149]

On the economic activity front, legislators have a safe harbor in Supreme Court precedent. The Court has frequently applied "laws regulating commerce to not-for-profit institutions," upholding labor measures, antitrust regulation, and more as applied to nonprofit entities.[150] In short, the "Commerce Clause is applicable to activities undertaken without the intention of earning a profit"—and the Court has found "no reason why the nonprofit character of an enterprise should exclude it from the coverage of either the affirmative or the negative aspect of the Commerce Clause."[151] It follows that a measure regulating a commercial activity—the use of consumer data—could be applied to charitable organizations without running afoul of the Supreme Court's new focus on narrowing the Commerce Clause.[152]

By carefully defining the scope of the federal preemptory measure to avoid the now-controversial "local activities" exception to *Lopez*'s Commerce Clause test, and through reliance on the Court's own jurisprudence in the area of nonprofit sector commercial regulation, Congress could implement an omnibus preemptory consumer data privacy measure that exempts charitable organizations from compliance.

C. Normative Concerns Support Federal Preemptory Action

Three normative arguments animate the case for a federal consumer data privacy measure that exempts charitable organizations. The first, a public policy case, rests on the public good done by

148. *But see Sebelius*, 567 U.S. at 563.

149. *See id.*

150. *See* Camps Newfound/Owatonna, Inc. v. Town of Harrison, 520 U.S. 564, 584-85 (1997) (summarizing applicability of commercial and economic regulations to nonprofit sector).

151. *See id.* at 584.

152. *See id.*

501(c)(3) organizations and the centrality of their operations to communities nationwide. The second case focuses on the lower potential of abuse of the data privacy exemption by (c)(3) organizations compared to their (c)(4) counterparts. The third argument maintains that the proper balance between the individual right to data control and data processing entities' survival lies in a measure that exempts only "true" charitable organizations, 501(c)(3) groups.[153]

1. Public Policy Favors Survival of 501(c)(3) Organizations

As the Smalltown Charity hypothetical illustrates, state-by-state consumer data privacy regulation jeopardizes nonprofit organizations' very survival. This problem is twofold. On one hand, the applicability thresholds of some states' privacy laws can capture (c)(3) groups regardless of income level, requiring compliance from even the tiniest of small-dollar organizations independent of their geographic locations.[154] On the other hand, the reality of (c)(3) budgetary constraints often places professional compliance counsel out of reach, which could cause these organizations to either comply as a default strategy (wasting resources unnecessarily—recall the Smalltowners) or to comply incorrectly (risking penalty).[155]

To reiterate the obvious from Part II of this Note (and via our Smalltown friends), the current state regulatory scheme in place is chaotic at best and impossibly contradictory at worst. Each measure outlined in Part II of this Note defines "personal information" (or "personal data") differently.[156] Each state law applies to a distinct collection of organizations—whether for- or nonprofit—and exempts a seemingly random set of entities.[157] The affirmative duties required under each statute vary wildly, and threatened penalties range from a proverbial slap on the wrist to a bankruptcy risk.[158] With a lack of uniformity across the states, *all* organizations

153. *See supra* Part III.B.
154. *See supra* Part II.
155. *See supra* Introduction, note 11 and accompanying text.
156. *See supra* Part II.
157. *See supra* Part II.
158. *See supra* Part II.

struggle with compliance—not just charitable entities with limited resources.

The challenges to good-faith compliance exist in the present state patchwork system and will only grow as more and more jurisdictions inevitably add their own patches to the metaphorical regulatory quilt.[159] While data on nonprofit organizations—(c)(3) or otherwise—that have been forced into bankruptcy on account of consumer data privacy requirements or penalties is currently nonexistent, a comparison of the fines imposed for failed compliance under the CCPA, VCDPA, and CPA against the average income levels of 501(c)(3) groups reporting to the Internal Revenue Service paints a clear mathematical picture: failure to comply with state consumer data privacy law could prove fatal.[160]

To effectuate the underlying public policy rationale of federal 501(c)(3) tax exemption—that charitable and educational organizations represent a societal good that the government wishes to encourage through the provision of a federal subsidy in the form of a tax exemption—consumer data privacy law should be federalized and crafted in a way that ensures 501(c)(3) survival. A federalized data policy with a (c)(3) carve-out would ensure that the aim of federal data privacy law as it pertains to 501(c)(3) organizations is aligned with the aim of federal tax policy: charitable and educational organizations would no longer have to deal with state-by-state chaos and would instead be granted a federal subsidy to ensure their continued survival.

In short, the "patchwork" of privacy measures currently in place is no doubt "patchy" and certainly does not work for the entities regulated. Creating a federal measure with a singular definition of personal data, a uniform scope of applicability, predictable compliance requirements, and a consistent infraction scheme would benefit *all* potentially regulated entities engaging in consumer data.

---

159. *See* Taylor Kay Lively, *US State Privacy Legislation Tracker*, INT'L ASS'N PRIV. PROS. (Mar. 31, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/K6DN-V73H] (noting that as of August 11, 2022, twenty-seven states have comprehensive privacy bills introduced, in committee, or on hold in the legislative process).

160. *See supra* Introduction, Part II.A.2-4.

2. Constraints on (c)(3) Activities Strengthen Case

Resistance to a 501(c)(3) exemption in consumer data privacy law is often presented in the form of a corruption or abuse concern—that is, a worry that certain types of organizations being exempted from a transparency-oriented policy will result in abuse of consumer data for the furtherance of nefarious activities.[161] This concern is particularly acute with so-called "dark money" nonprofit organizations.[162] "Dark money" groups are those that have wide discretion on their advocacy, political, and electoral activities, and have little to no corresponding disclosure obligations to governmental regulators.[163] Exempting such organizations from yet another transparency-oriented measure, so the argument goes, positions nonprofit groups to exploit consumer data for political aims with impunity and free of enforcable repercussions.

This concern is no doubt relevant to certain classifications of tax-exempt entities but fundamentally misunderstands the constraints already in place on 501(c)(3) activity. Organizations classified as public charities under I.R.C. section 501(c)(3) are completely prohibited from engaging in electoral activity: they may not support or oppose candidates for election, indirectly or directly, monetarily or otherwise.[164] 501(c)(3)s are also heavily limited in their ability to influence legislation, often called lobbying, and may not make lobbying-related activity a "substantial part" of their operations.[165] Violating either of these provisions is grounds for revocation of exemption.[166]

---

161. This concern is generally more prevalent in the for-profit sector. Given the focus of this Note, only the limited relevance of this concern to 501(c)(3) organizations will be discussed.

162. *See* Chisun Lee & Daniel I. Weiner, *Dark Money*, BRENNAN CTR. FOR JUST. (2021), https://www.brennancenter.org/issues/reform-money-politics/influence-big-money/dark-money [https://perma.cc/Q9WH-HTG4] (providing overview of the over $1 billion spent in federal elections since 2010, from 501(c)(4)-exempt groups and other disclosure-free organization types).

163. *See id.*

164. I.R.C. § 501(c)(3) (defining permissible (c)(3) purposes and stating that such organizations must "not participate in, or intervene in ... any political campaign").

165. *Id.* "No substantial part" has never been explicitly defined by the IRS. Note that organizations classified as private foundations under section 501(c)(3) may not lobby at all. *See generally* I.R.C. § 4945.

166. *See* I.R.C. § 501(c)(3).

Combined with the overarching prohibition that the 501(c)(3) business structure may not be used to generate net earnings for private persons, these explicit lobbying and political prohibitions substantially limit—if not entirely curb—the amount of data-driven nefarious activity that 501(c)(3) organizations could conduct if exempted from a federalized data privacy measure.[167] The behavioral restraints operative in the federal tax code therefore counterbalance the corruption concern that motivates some against a 501(c)(3) consumer data privacy exemption.[168]

3. Balance of Individual Right vs. Nonprofit Existence

Exempting 501(c)(3) groups from compliance with a federalized consumer data privacy measure properly balances the individual right of control over personal data against the public good of charitable and educational organizations encouraged by federal tax policy.

A federalized policy without a 501(c)(3) exemption would swing the privacy pendulum too far in favor of individual data control rights at the expense of the nonprofit sector.[169] As discussed in the Introduction of this Note, leaving 501(c)(3) organizations caught in the confusion of consumer data privacy compliance tangibly risks the bankruptcy of charitable organizations for the vindication of consumer data rights. By contrast, an exemption that captures all federally tax-exempt entities (such as an exemption that extends to trade associations and lobbying organizations) would improperly weigh noncharitable groups' business interests over individual consumer data rights.[170]

The optimal balancing of these competing interests—the individual right to data privacy held by a consumer and the societal interest in the continued existence of charitable and educational

---

167. *See id.*; *supra* notes 161-66 and accompanying text.

168. *See supra* notes 161-66 and accompanying text. The narrowness of the consumer data privacy exemption serves as yet another barrier against abuse: 501(c)(4) organizations, the archetypical "dark money" nonprofit structure, would be required to comply with the hypothesized preemptory measure.

169. *See generally supra* Introduction (discussing hypothetical (c)(3) bankruptcy due to consumer data privacy compliance).

170. *See supra* Part III.C.2.

organizations—is found in exempting *only* 501(c)(3) organizations from a federalized data privacy measure.[171] The same public policy rationales discussed in the Introduction and Part III.C.1 of this Note do not apply to non-501(c)(3) exempt organizations because the "public good" served by non-(c)(3)s (if it can be termed that at all) is intrinsically different from the public good fostered by charitable and educational entities.[172] Without a greater societal good to justify an infringement on the individual right to data privacy,[173] the rationale for exempting any type of business structure from compliance with a privacy measure falls away.[174]

The proper balance between individual and societal rights in a comprehensive, preemptory federal consumer data privacy scheme is therefore one that exempts solely 501(c)(3) organizations from compliance.

IV. STATES DO NOT KNOW BEST

Three main counterarguments are likely to be proffered against the idea of a federal omnibus consumer data privacy measure that exempts 501(c)(3) organizations. The first two were dispelled by Part III of this Note: the ideas that exempting 501(c)(3) organizations from compliance would (1) encourage corruption and (2) improperly favor societal good over individual rights do not hold water when considered within the framework of existing tax code-imposed behavioral constraints and the narrowness of the exemption being proposed.[175]

The last argument against such a preemptory, exemption-providing measure sounds a familiar refrain: the Tenth Amendment

171. *See supra* Part III.C.

172. *Compare, e.g.*, I.R.C. § 501(c)(3) (exempting charitable and educational groups from federal income tax), *with, e.g.*, I.R.C. § 501(c)(6) (exempting trade associations from federal income tax).

173. The "infringement" in this sense would be the exemption of a single type of entity from compliance, effectively meaning there would be a business structure against which an individual would not be able to vindicate their data rights.

174. *But see supra* Part III.C.1 (discussing societal good that underlies argument for exempting 501(c)(3) organizations).

175. *See supra* Part III.C.2-3.

and state expertise.[176] With multiple states already stepping in with comprehensive, high-quality consumer rights legislation, what good would uniform federal action serve when faced with diverse consumer bodies nationwide? So the argument goes: it is an individual state legislature's prerogative to choose to exempt 501(c)(3) organizations from—or obligate them to ensure—consumer data privacy compliance, and this policy directive should not be unilaterally imposed on jurisdictions that have unique consumer needs—and that are "closer" to the subjects of regulation when compared to the federal government.

Like the case for federal preemptory action exempting 501(c)(3)s outlined in Part III of this Note, this Tenth Amendment-*esque* position is easily countered with a look at normative arguments that dispense with state efficiency and expertise. First, the 501(c)(3) income tax exemption is created and administered by the federal government.[177] It would maximize efficiency for charitable organizations that are recognized by the federal Internal Revenue Service to have their privacy law exemption administered at the same governmental level.[178]

Second, the idea that states are more adept at regulating entities in this area is strongly rebuffed by the number of revisions that existing state law has already required before going into effect.[179] For example, Virginia's Act required the creation and review of a special "Work Group" before the Act's implementation in January 2023.[180] The Group's Final Report, generated over the course of six meetings, recommended at least twelve concrete, nontrivial revisions to the bill—including its definition of sensitive data, its right to deletion, and its enforcement mechanisms—before the measure is scheduled to take effect.[181] These recommendations cut at the substantive heart of the VCDPA and are emblematic of the

176. *See generally* U.S. CONST. amend. X (generally reserving powers not granted to the federal government for the states).

177. *See generally* I.R.C. § 501(c)(3).

178. Since the federal government maintains a database of 501(c)(3)-exempt organizations, it would presumably be more straightforward for it to administer another statutory exemption that hinges on this status compared to another governmental entity (such as a state).

179. *See, e.g.*, VA. CODE ANN. § 59.1-581.2 (effective Jan. 1, 2023) (second passage).

180. VA. JOINT COMM'N ON TECH. & SCI. VA. CONSUMER DATA PROT. ACT WORK GRP., 2021 FINAL REPORT 1 (2021).

181. *Id.* at 2.

greater pattern seen across state privacy legislative processes: states simply do not possess the expertise to "get it right" on the first time through.

In an area with such substantial compliance costs, "getting it right"—up front, and not years later—is crucial.[182] While states may be effective laboratories of experimentation in other legislative realms, in the world of privacy law, they are more akin to a mad scientist's lair, with a piecemeal policy more resembling Frankenstein's monster than elegant creation.

Finally, states are not closer to their subjects of regulation, data-holding entities, in a way that often justifies state policy making over federal regulation. Entities that are regulated by consumer data privacy laws, whether for- or nonprofit, are inherently internet based and without borders.[183] Unlike a local agricultural industry (say, growing oranges), which constitutes a group of businesses intrinsically tied to physical and state-based land, internet-based businesses are no closer to a state's government than they are to the federal bureaucracy. While a state may have more specialized knowledge to regulate the local citrus fruit community by virtue of the orange groves being physically located within state lines, the state does not possess the same localized, innate knowledge when it comes to businesses operated in cyberspace.

The Tenth Amendment-style arguments against federal preemption are therefore not maintainable on either efficiency or expertise grounds. When viewed in conjunction with the counterarguments raised against and dispensed with for the 501(c)(3) exemption specifically, the strength of the proposed federal legislative solution speaks for itself.

CONCLUSION

Congress should use its Commerce Clause power to pass a comprehensive, preemptory federal consumer data privacy measure that explicitly exempts 501(c)(3) organizations from compliance. This legislation would properly balance the public policy benefit achieved

182. *See generally supra* Introduction, Part I.

183. *See, e.g.*, *supra* Introduction (discussing the Smalltowners).

by the existence of 501(c)(3) organizations against the growing calls for universal consumer data privacy rights and corresponding increased burden on nonprofit entities covered by states' privacy regimes.

Such a uniform system would mend the patchwork of the three state measures currently in existence, under which each state implements a different scope of applicability, a unique compliance requirement checklist, and varying enforcement mechanisms and penalties. Given the current digital marketplace, in which even small organizations are captured by differing privacy laws that extend past state lines and into the ether, relegating this policy area to the states is plainly inadequate for an increasingly online economy. As an indisputably commerce-oriented measure to govern the entire United States economy, it is exclusively the province of the federal legislature to institute a singular consumer data privacy regime nationwide.

Charitable organizations exempt from federal income tax under section 501(c)(3) of the Internal Revenue Code ought to be exempt from such a preemptory measure. The 501(c)(3) exemption is a legislative recognition of the public good done by organizations committed to charitable and educational missions. Simultaneously, the nature of the 501(c)(3) regulations all but requires charitable groups to deal in data for their continued existence. Unlike the for-profit world, charitable groups are less capable of following the prescriptions of the patchwork due to limited financial, personnel, and technological resources—despite their being subject to the same compliance obligations as profit-generating entities.

Congress—and the public at large—has a unique interest in sustaining the Smalltown Charities of America, in establishing a federal omnibus consumer data privacy measure that excuses 501(c)(3)-exempt organizations from compliance.

Smalltown Charity could someday become Newtown Charity, a successor organization situated in Big Country, a nation that has passed a federal data measure with plain language that clearly exempts Newtown Charity from compliance. Newtown Charity would be able to continue operations until its mission is achieved: Newtown has transitioned away from coal, its community is sustainably powered, and its people are well.

While the loss of Smalltown Charity alone may appear as a singular missing square on the quilt of nonprofit organizations that covers the country, the current system of state consumer data privacy measures threatens to unravel *this* patchwork—that of small-donor, big-impact charitable and educational organizations—entirely.

Sarah Fisher[*]

* J.D. Candidate 2023, William & Mary Law School; B.A. 2016, Foreign Affairs, University of Virginia (go Hoos). Thank you to each William & Mary Law Review member who thoughtfully reviewed my Note for details as small as a mis-italicized comma, and a special thanks to Daniel Ruesta for helping the Smalltowners come to life. I am grateful to Holly Ratliff for giving me a two-paragraph assignment that somehow turned into 7,000 words and to my parents for always reminding me to eat an elephant (or draft a Note) one bite at a time. Finally, to CB, my favorite physicist and #1 cheerleader: two hand squeezes and a third.