PETITIONS, PRIVACY, AND POLITICAL OBSCURITY

Rebecca Green[*]

People who sign petitions must accept disclosure of their political views. This conclusion rests on the seemingly uncontroversial (if circular) premise that petition signing is a public activity. Courts have thus far shown little sympathy for individuals who take a public stand on an issue by signing a petition and then assert privacy claims after the fact. Democracy, after all, takes courage, as Justice Scalia wrote in the petitioning disclosure case Doe v. Reed*. But signing a petition today brings consequences beyond public criticism. The real threat of disclosure for modern petition signers is not tangible harassment, but the loss of "political obscurity" in a modern data architecture that exposes citizens to indelible Internet scrutiny and rampant political preference cataloguing. This Article argues that political obscurity is an important, unarticulated interest in the current discourse about privacy and petitioning. Courts and state administrators must take steps to protect it or risk drastically diminished participation in petition signing. Finally, this Article suggests that political obscurity has important implications in other areas of political participation. For example, those who contribute small amounts to political campaigns and petition signers may share a similar privacy interest. "Drop-in-the-bucket" political gestures ought not extinguish political obscurity.*

I. INTRODUCTION

A citizen's right to petition the government has a long pedigree. Likewise, courts and commentators have flagged the right to privacy for decades. Until recently, the two rights coexisted. In the digital age, however, as our zones of privacy constrict, political privacy faces an assault from petitioning norms (and court opinions) that fail to acknowledge new technological realities. Perhaps the assault on political privacy will not threaten petitioning activity. Maybe citizens will continue signing petitions even when doing so today may radically expand exposure of their political preferences. But if political privacy does matter, if the reaction to amplified exposure in petition signing does dissuade people from signing petitions, a basic part of our political process will be threatened.[1] If political privacy does matter to petition signers, failure to protect it

* Professor of Practice, William & Mary Law School; Co-Director, Election Law Program (a joint project of William & Mary Law School and the National Center for State Courts). The author would like to thank Neal Devins, Vivian Hamilton, Alli Orr Larsen, Tim Zick, Laura Heymann, and Rick Hasen. A special thanks also to Jonathan Zittrain and participants at the 2012 Cyberlaw Colloquium for their insights, ideas, and encouragement. Finally, I would like to thank Megan Mitchell for her incredible research abilities and thoughtful contributions.

1. *Cf.* Raymond J. La Raja, *Does Transparency of Political Activity Have a Chilling Effect on Participation?* 1 (2011) (Paper presented at the Annual Meeting of the Midwest Political Science Association, Mar. 31–Apr. 3, 2011), *available at* http://projects.iq.harvard.edu/cces/publications/does-transparency-political-activity-have-chilling-effect-participation (arguing that decreasing anonymity has a chilling effect on

could take the legs out from underneath a right so central to our democratic construct that it is enshrined by name—unlike the right to privacy—in the text of the First Amendment.

The modern battlefield for privacy rights in petition signing has been waged most prominently over same-sex marriage petitions and whether or not signers must "out" their political views to their communities when they sign petitions against gay marriage. The leading case is *Doe v. Reed*,[2] in which Washington State anti–gay marriage petition signers tried to prevent the release of their names after several organizations sought access to the filed petition through the state's Public Records Act.[3] Activists circulated the petition, R-71, to repeal by public referendum a newly minted law, which expanded the rights of same-sex couples.[4] The plaintiffs worried when ominously named organizations like WhoSigned.org and KnowThyNeighbor.org signaled intent not only to publish petition signers' names and home addresses online, but also attach home phone numbers and online maps providing directions to petition signers' homes.[5] The plaintiffs feared this targeted Internet dissemination would "effectively become a blueprint for harassment and intimidation."[6] The *Reed* plaintiffs likened this threat to that faced by members of the National Association for the Advancement of Colored People (NAACP) during the Civil Rights Era in a case that involved exposure of its membership lists.[7]

The comparison came under fire in scholarly circles and in the media.[8] The harms

political participation).

2. 130 S. Ct. 2811 (2010).

3. WASH. REV. CODE ANN. §§ 42.56.010–42.56.904 (West 2012). Referendum proponents must file a petition with the Secretary of State containing valid signatures of registered Washington voters "equal to or exceeding four percent of the votes cast for the office of governor at the last gubernatorial election." WASH. CONST. art. II, § 1(b), (d). "A valid submission requires not only a signature, but also the signer's address and the county in which he [or she] is registered to vote." *Reed*, 130 S. Ct. at 2816 (citing WASH. REV. CODE ANN. § 29A.72.130).

4. *Reed*, 130 S. Ct. at 2816. The effort ultimately failed and voters approved the law by a margin of fifty-three percent to forty-seven percent. S. 5688, 62nd Leg., Reg. Sess. (Wash. 2011).

5. *Id.* at 2816, 2820; Jessica Geen, *Groups Threaten to Publish Names of US Gay Rights Opponents*, PINKNEWS (June 9, 2009, 11:53 AM), http://www.pinknews.co.uk/2009/06/09/groups-threaten-to-publish-names-of-us-gay-rights-opponents/; Carlos Santoscoy, *Gay Rights Group To Post Names Of R-71 Petition Signers*, ON TOP (Oct. 19, 2011), http://www.ontopmag.com/article.aspx?id=9834&MediaType=1&Category=26#.

6. *Reed*, 130 S. Ct. at 2820.

7. *See* Brief for Petitioner at 32, *Reed*, 130 S. Ct. 2811 (No. 09-559), 2010 WL 711186 (arguing district court error for failure to consider the problem of government "facilitation of intimidation by compelling disclosure" as articulated in *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 463 (1958)).

8. For example, Joseph Birkenstock, an attorney at Caplin & Drysdale and former chief counsel of the Democratic National Committee, noted the traditionally high harassment bar set at the start of the civil rights era, when those who fought disclosure feared being hanged. Explained Birkenstock:

> If you look at the disclosure exemptions that have been recognized in the past . . . like for the NAACP in Alabama in 1957, ... [y]ou had strange fruit hanging from Southern trees. That's not happening now.
>
> . . . I'm not arguing in favor of harassment, but I'm just saying there is kind of a continuum that has been present in the past that isn't there today.

Michael Beckle, *Court Battles over Campaign Finance Disclosure Loom, Legal Experts Predict*, OPEN

befalling civil rights activists were real, including loss of employment and all-too-imminent threats to physical safety.[9] In 2010, anti–gay marriage sentiment was barely a minority view in Washington State; the risks of harm were speculative.[10] Thus, it came as no surprise when the Court proclaimed that the plaintiffs failed to demonstrate harm according to the formula developed in *NAACP v. Alabama ex rel. Patterson*[11] over fifty years ago: a "reasonable probability that the compelled disclosure [of personal information] will subject them to threats, harassment, or reprisals."[12] In the eight to one opinion, only Justice Thomas found the threat of harassment to the Washington petition signers facially compelling.[13] Justice Scalia, in a concurring opinion, admonished that signing a petition is a "political act[] [that] fosters civic courage." [14] Without civic courage, Scalia warned, "democracy is doomed."[15]

A year later, on remand, the as-applied challenge met a similar fate.[16] Plaintiffs tried to muster examples of requisite threats and harassment under the *NAACP* test, but the federal district court found the evidence lacking.[17] One plaintiff, Matthew Chenier, testified that when he waved an anti–gay marriage banner in a high-traffic area he got an angry text message from his brother, and an unidentified passenger in a passing car "mooned" him.[18] Dmitry Kozlov testified that while gathering signatures, a man "directed expletives at him and pushed him;" that another man, "threw garbage at [his] group from a van" (no injuries reported); that a woman told him "we'll do everything to stop what you're doing;" and that another man said "we'll have your kids."[19]

Whatever one thinks of the gravity of these asserted harms as a harbinger of what might transpire upon public release of signatures, an odd fact remains: not a single plaintiff or witness in the as-applied challenge shied from using their real names in the suit.[20] In a case suing to protect the privacy of petition signers, there was a notable lack

SECRETS BLOG (March 20 2011, 10:27 AM), http://www.opensecrets.org/news/2011/03/court-battles-over-campaign-disclos.html (quoting Joseph Birkenstock).

9. In *NAACP v. Alabama ex rel. Patterson*, given the sustained violence against African American civil rights activists in the South, the Supreme Court accepted the "uncontroverted showing that on past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." 357 U.S. at 462.

10. Voters in Washington were nearly equally divided on the issue. *See Reed*, 130 S. Ct. at 2816 ("The voters approved SB 5688 by a margin of 53% to 47%.").

11. 357 U.S. 449 (1958).

12. *Reed*, 130 S. Ct. at 2820 (quoting Buckley v. Valeo, 424 U.S. 1, 74 (1978) (per curiam)). The *Buckley* Court explained that this standard can be met upon a showing of the type harassment that occurred in *NAACP*, which included "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." *Buckley*, 424 U.S. at 69.

13. *Reed*, 130 S. Ct. at 2838 (Thomas, J., dissenting).

14. *Id.* at 2837 (Scalia, J., concurring).

15. *Id.*

16. Doe v. Reed, 823 F. Supp. 2d 1195, 1212–13 (W.D. Wash. 2011).

17. *Id*. at 1204–10.

18. *Id*. at 1205.

19. *Id*. at 1207.

20. For example, Plaintiff Richard Long stated that he had "no problem testifying publicly in this matter" and that his involvement with the petition drive against gay marriage in Washington "need not be kept secret." *Id*. at 1206.

of concern about the actual plaintiffs' or witnesses' privacy. Quite to the contrary, virtually all of the plaintiffs and witnesses were vocal and public opponents of gay marriage.[21] Plaintiff Ronald Perkins (named in the suit as "John Doe #1" despite his willingness to use his real name), for example, shouted his opposition to same-sex marriage far and wide in an Internet video.[22] Roy Hartwell ("John Doe #4") testified about the petition before the Washington State Legislature, gathered signatures for the petition in public places, and participated in television interviews regarding the effort.[23] Pastor Ken Hutcherson, a long-time opponent of gay marriage, testified that Googling his name "results in approximately 300,000 hits related to his stance opposing gay marriage."[24] The individuals that the *Reed* plaintiffs used to document "harm" all took a very public stance on gay marriage. Is it any wonder that plaintiffs' call for privacy in petition signing rung hollow?

The *Reed* plaintiffs and witnesses were outspoken public opponents of gay marriage for a reason: the plaintiffs' only hope to satisfy the *NAACP* standard required cataloguing the harms that befell opponents of gay marriage—those at the public heart of the debate.[25] But the strategy proved problematic. It is difficult to muster sympathy for the *Reed* plaintiffs' privacy interests after they made their political beliefs so publicly known. If one holds a politically provocative sign on a crowded sidewalk and gets mooned by those who disagree with its content, one should expect no less; after all, democracy takes courage.[26]

The privacy interests of those who hold their political views closer to the vest are missing from the *Reed* narrative. What if the real (and much more difficult to document) harm befell those who did not—or would not—sign the petition? What if the harm in releasing petition names is not to activists being mooned or shouted at as they advocate publicly for their cause? What if the real privacy victim is a mother of two, passing a petition circulator entering the grocery store, fearful that signing a petition—even for a cause in which she very much believes—might create a lifelong indelible association with that cause on her Internet record? In applying a harassment-based harm standard lifted from the 1950s, courts miss the very real and changed nature of the privacy problems petition signers (actual or prospective) face today.

At first glance, it may be hard to muster sympathy for political privacy in the Internet Age. Throngs of Americans undertake online political activism every day. The Internet enables mass mobilization of political sentiment on an unprecedented scale.[27] Yet, as our political identities are increasingly exposed online, the act of signing an official petition has real—and lasting—privacy consequences. In an era of radically

21. *See id.* at 1205–10 (listing opponents to gay-marriage referendum and their actions in opposition).

22. *Id*. at 1205.

23. *Id*. at 1206.

24. *Id*. at 1206–07.

25. *See id.* at 1199 (describing the "Exacting Scrutiny" standard required for the plaintiffs' claim).

26. *See* Doe v. Reed, 130 S. Ct. 2811, 2837 (2010) (Scalia, J., concurring) ("Requiring people to stand up in public for their political acts fosters civic courage, without which democracy is doomed.").

27. *See* Molly Beutz Land, *Networked Activism*, 22 HARV. HUM. RTS. J. 205, 218–20 (2009) (providing examples of online activism); Seth F. Kreimer, *Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet*, 150 U. PA. L. REV. 119, 121 (2001) (describing how the Internet has developed into the dominant form of communication and organization for social movements).

expanded exposure, petition signers today experience a deeply troubling loss of what this Article terms "political obscurity." Until very recently, those who wanted to shield their political preferences from broad exposure could rely on an information architecture that made it very difficult for the political views of ordinary citizens to be exposed on a broad scale.[28] The vast majority of citizens, in other words, enjoyed political obscurity. No more. Technology threatens political obscurity in ways that backwards-looking courts and legislators have largely failed to appreciate.

This Article proceeds in three parts. Section II introduces the concept of political obscurity, laying out its basic parameters and situating it in the scholarly dialogue about information privacy in the digital age. Section III analyzes the danger that modern technology poses to political obscurity. Section IV examines petitioning in the United States, outlining its modern incarnations with particular attention to the information architectures and privacy protections (or lack thereof). Section V makes the normative claim that courts, legislators, and state administrators should take steps to protect political obscurity in petitioning, suggesting a path forward to ensure transparency in the petitioning process without sacrificing vital political privacy rights. Finally, this Article concludes that recognizing a right to political obscurity for small-scale political acts has broader application.

II. POLITICAL OBSCURITY

Political obscurity refers to individual control over the scope of public knowledge about one's political preferences.[29] As democratic citizens, we all have various tolerances for exposing our political views to others.[30] Some prefer to make their personal political views well known, whether it is plastering their cars with bumper stickers, standing on street corners with signs, or blogging on forums under their real names. Most, however, prefer to keep some (or all) political views private.[31] Whether

28. *See* William McGeveran, *Mrs. McIntyre's Persona: Bringing Privacy Theory to Election Law*, 19 WM. & MARY BILL RTS. J. 859, 863 (2010) ("[T]he changing nature of journalism and the maturation of the internet continue to intensify the effect of disclosure on ordinary political participants.").

29. This is a play on the term "practical obscurity." For a review of the phenomenon of practical obscurity in the court records context, see Peter A. Winn, *Judicial Information Management in an Electronic Age: Old Standards, New Challenges*, 3 FED. CTS. L. REV. 135, 152–53 (2009), and *infra* Section V. Deborah Johnson, Priscilla Regan, and Kent Wayland define practical obscurity as "the work involved in obtaining access and duplicating information [with] . . . the effect of protecting the privacy of the information." Deborah G. Johnson et al., *Campaign Disclosure, Privacy and Transparency*, 19 WM. & MARY BILL RTS. J. 959, 960 (2011). They continue, "[i]n the networked world, those built-in protections are removed and there is little or no obscurity. Records can be easily accessed, searched, analyzed, and reconstituted in new forms from nearly anywhere in the world." *Id.*

30. According to a study published in 1996, less than one percent of surveyed cars displayed at least one bumper sticker declaring support for or identification with a political group. James W. Endersby & Michael J. Towle, *Tailgate Partisanship: Political and Social Expression Through Bumper Stickers*, 33 SOC. SCI. J. 307, 314 (1996); *see also* David J. Koch & Douglas V. Porpora, *Political Bumper Stickers and Vehicle Class: Are SUVs the Enemy?*, *in* SIGNS OF WAR: FROM PATRIOTISM TO DISSENT 17, 20 (Anne-Marie Obajtek-Kirkwood & Ernest A. Hakanen eds., 2007) ("[I]n the United States, political messages constitute a relatively marginal percentage of all bumper stickers.").

31. *See* James A. Gardner, *Anonymity and Democratic Citizenship*, 19 WM. & MARY BILL RTS. J. 927, 943 (2011) (discussing the advent of the secret ballot as a mechanism "to enhance citizen independence and

the preference for political obscurity is professional, personal, or cultural, most Americans do not display political bumper stickers and do not stand on street corners with signs.[32]

The term political obscurity imports into the political context a concept initially developed to describe privacy protections built into pre-Internet court records systems by virtue of the practical difficulty of accessing paper court records.[33] The Supreme Court first recognized "practical obscurity" in the 1981 case *United States Department of Justice v. Reporters Committee for Freedom of the Press*.[34] In *Reporters Committee*, the Court found that CBS News did not have a right of access under the Freedom of Information Act (FOIA)[35] to a federal criminal "rap sheet" of Charles Medico, an individual under media scrutiny for alleged mob activities.[36] The sought-after information could be located in public court records, documents that CBS could have retrieved with great time, money, and effort by searching through dusty court files in courthouses across the country.[37] But the federal government maintained computerized criminal records database containing Medico's criminal history records in one convenient place.[38] *Reporters Committee* examined whether Charles Medico possessed a right to "practical obscurity" that would preclude the media from easy access to state-held criminal information about him.[39] The Court found in Medico's favor, acknowledging that technology dramatically impacted the privacy interests at issue.[40] Wrote Justice Stevens, "both the common law and the literal understandings of privacy

sincerity by freeing voters to vote their actual preferences rather than those of a party to which they felt beholden or that they feared"). Many of us share this preference. Echoing my own sensibilities, election law scholar James Gardner writes of the prospect of having his own political preferences being broadcast on the Internet, "I don't like that at all." *Id.* at 927.

32. Or even vote, as signaled by the low voter turnout in the United States compared to other developed democracies. *See* Rafael Lopez Pintor et al., *Voter Turnout Rates from a Comparative Perspective*, *in* VOTER TURNOUT SINCE 1945: A GLOBAL REPORT 75, 78–79 fig. 11 (2002) (ranking the United States 120th internationally in voter turnout between 1945 and 2001; averaged over seventeen elections).

33. *See* Winn, *supra* note 29, at 152 (noting that while records in a pre-Internet, paper-based system are technically public, it offers a considerable amount of protection based on the "sheer difficulty of accessing it"). For a detailed definition of the term "political obscurity," see *infra* Part II.A.

34. 489 U.S. 749 (1989). Nancy Marder examined the relevance of *Reporters Committee* in the political context, specifically comparing court records and campaign finance disclosure. Nancy S. Marder, *From "Practical Obscurity" to Web Disclosure: A New Understanding of Public Information*, 59 SYRACUSE L. REV. 441, 441–43 (2009).

35. 5 U.S.C. § 552 (2006).

36. *Reporters Comm.*, 489 U.S. at 762–63.

37. *Id.* at 764.

38. The dissenting judge in the circuit court recognized the distinction between gathering information through hardcopy court files and computerized databases when he noted, "computerized data banks of the sort involved here present issues considerably more difficult than, and certainly very different from, a case involving the source records themselves." Reporters Comm. for Freedom of the Press v. U.S. Dep't of Justice, 831 F.2d 1124, 1128 (D.C. Cir. 1987) (Starr, J., dissenting), *rev'd*, 489 U.S. 749 (1989).

39. *Reporters Comm.*, 489 U.S. at 762. Notably, *Reporters Committee* was not a constitutional case. Medico's privacy interests were expressed by FOIA's exemption 7(C) which excludes records or information compiled for law enforcement purposes, "but only to the extent that the production of such [materials] . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy." *Id.* at 756 (alteration in original) (quoting 5 U.S.C. § 552(b)(7)(C)).

40. *Id.* at 764.

encompass the individual's control of information concerning his or her person."[41] Stevens continued: "The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded."[42]

The concept of *political* obscurity introduced here builds on the *Reporters Committee* understanding of Mr. Medico's privacy interest. It has long been recognized that some measure of privacy is required for democracy to function.[43] I argue that political obscurity is an essential component of that function. The Parts that follow describe political obscurity, provide examples of the Supreme Court's recognition of the right in First Amendment jurisprudence, and explore its fate in the Court's petitioning cases.

A. The Contours of Political Obscurity: What It Is and What It Isn't

The nature of political obscurity has never been fully examined; the concept has never, to this Author's knowledge, been formally identified or defined.[44] This Part will therefore endeavor to establish its parameters and identify its scholarly precursors.

Political obscurity refers to the state of one's political preferences being shrouded or otherwise difficult to discern or distinguish by others. A person enjoys political obscurity when she can go about her day as she so chooses without others perceiving or otherwise determining the nature of her political views. The politically obscure person is able to control and manage the extent of disassociation from the political views she holds (or once held) or political actions taken in the present and in the past.

Political obscurity is related to, but broader than, anonymity. We have long understood political anonymity to describe the masking of one's identity in political discourse. Political obscurity may be accomplished through the use of anonymity—masked identity on chosen political platforms (online or in the real world). But throughout history most people enjoyed political obscurity without masking their identities. Political obscurity is far more commonly achieved by choosing not to share political views at all, or by sharing in a purposefully limited sphere enabled by an information/data poor environment.[45] Political obscurity therefore describes a broader right than anonymity: it is the fundamental right to exist without one's political preferences being continuously recorded and, consistent with the right articulated in

41. *Id*. at 763.

42. *Id*. at 771.

43. *See* JOHN STUART MILL, ON LIBERTY AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT 4 (R. McCallum ed., 1946) (observing that while public expression of political opinion is a hallmark of democracy, some privacy is needed in order to prevent the government from oppressing those with certain political views); ALAN F. WESTIN, PRIVACY AND FREEDOM 24 (1967) ("Just as a social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies.").

44. That said, numerous observers have acknowledged that the modern information landscape fundamentally changes the privacy landscape for ordinary political actors. See *infra* notes 57–60 and accompanying text for further discussion on the Internet's impact on behavior in the real world.

45. McGeveran, *supra* note 28, at 863.

Reporters Committee, a right against state-facilitated cataloguing of one's political preferences.

One's preference for political obscurity need not be absolute. Citizens may desire or expect to remain politically obscure on some issues but not others. A vocal critic of the war in Afghanistan, for example, may prefer her views on abortion remain private. Political obscurity is likewise not the same thing as a desire for total secrecy of one's political positions. One's political preferences may be well known to family and friends, larger groups within one's community, or even one's whole geographic locality.[46] A person suffers a loss of political obscurity, however, if she were forced to reveal her political preferences in spheres in which—had she total control—she would choose not to.[47]

Time affects political obscurity. Political obscurity can be achieved not just by confining the scope of one's political activities, but also by the natural passage of time through which one's public political activities fade and are forgotten.[48] Until recently, time served as a reliable means of ensuring individual political obscurity.

The observation of technology's threat to political obscurity grows out of a vigorous privacy dialogue scholars have engaged in since the rise of the networked world. When the Internet arose, scholars immediately recognized its potential as a rich new platform for democratic debate.[49] But scholars quickly recognized the downsides: technology's erosion of personal privacy and the potential for that erosion to chill political speech.[50] Early observation focused predominantly on the Internet itself as a potential forum for democratic discourse.[51] Would this new space replace or re-energize the public square? As these discussions unfolded, observers identified online privacy as a threat to this new deliberative space.

Paul Schwartz, one of the first such commentators, wrote *Privacy and Democracy in Cyberspace* in 1999. Schwartz noted that political participation in the real world is not like political participation online: on the Internet, a digital record of your online

46. By "community" here, I am not necessarily referring to community in a geographic sense. Indeed, one's community in the modern world can include far-flung individuals one has never met.

47. One illustrative example that comes to mind is Oliver Sipple. In 1975, Sipple prevented Sarah Jane Moore from assassinating President Ford in San Francisco. Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665, 666 (Ct. App. 1984). The San Francisco Chronicle and other news outlets ran stories about his heroic act. *Id.* The articles identified Sipple as a prominent member of San Francisco's gay community, a fact Sipple had not shared with his family back home in Detroit. *Id.* Sipple sued, asserting tort violation of his privacy through publication of private facts about him. *Id.* at 667. The court was unsympathetic, noting that "there can be no privacy with respect to a matter which is already public." *Id.* at 669. Sipple fell prey to a loss of relative obscurity.

48. This temporal aspect of practical obscurity in the court records context carried the day in *Reporters Committee*, where the Court noted that "the ordinary citizen surely has a similar interest in the aspects of his or her criminal history that may have been wholly forgotten." 489 U.S. at 769.

49. *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1648 (1999) (indicating that "[c]yberspace has the potential to emerge as an essential focal point for communal activities and political participation").

50. *See id.* at 1647–53 (analyzing how privacy concerns on the Internet will discourage participation and deliberation in democracy).

51. *Id.* at 1650.

movements is recorded.[52] According to Schwartz, preserving the Internet as a truly open marketplace of ideas would require rules that maintain some measure of control over one's digital footprints.[53]

The following year, Julie Cohen echoed the theme, advocating for individuals' control over information about them online. Cohen noted that individual autonomy plays a central role in development of democratic personhood.[54] Cohen was concerned that a "no privacy" environment would hamper informed and deliberate self-governance online.[55] A robust debate, she wrote, "requires the opportunity . . . to keep distinct social, commercial, and political associations separate from one another."[56] Early observers like Cohen and Schwartz zoomed in on the need for individual autonomy and control of personal information in cyberspace.

Later, scholars began to address the Internet's impact on behavior in the real world. Daniel Solove, in his 2007 book *The Future of Reputation*,[57] recounted a vivid example: a girl on a Korean subway who neglected to clean up after her dog faced real consequences when a video of her lapse went viral online.[58] Our right to control information about us, Solove observed, is exacerbated by the free speech rights of others and the free flow of information online.[59] Solove's work underscored the impact of this phenomenon on democratic discourse. Those who feel nervous about overexposure of political views, he noted, might refrain from engaging in democratic debate.[60]

Wrestling with the problem Solove and others identified, scholars and policymakers have been toying with the idea that the right to control information about us extends to the right to delete. In his 2009 book on the subject, Viktor Mayer-Schönberger argued: "As digital memories make possible a comprehensive reconstruction of our words and deeds, even if they are long past, they create not just a spatial but a temporal version of Bentham's panopticon, constraining our willingness to say what we mean, and engage in our society."[61] Mayer-Schönberger's solution is to invoke an individual right to delete information stored about us—online and

52. *Id.* at 1651 ("Listening to ideas in Real Space generally does not create a data trail, listening on the Internet does.").

53. Schwartz used the term "self-determination" to describe individual control of data regarding their identity. *Id.* at 1653. Self-determination, he wrote, "should be defined as people who, as part authors of their lives, substantially shape their existence through the choices they make." *Id*. at 1655.

54. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STAN. L. REV. 1373, 1425 (2000) ("[T]he benefits of informational autonomy (defined to include the condition in which no information is recorded about nonanonymous choices) extend to a much wider range of human activity and choice . . . . The opportunity to experiment with preferences is a vital part of the process of learning, and learning to choose, that every individual must undergo.").

55. *Id*. at 1426–27.

56. *Id*.

57. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION (2007).

58. *Id.* at 1–4.

59. *Id.* at 2.

60. *Id.* at 131.

61. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 197 (2009).

elsewhere.[62] This call for digital forgetting has resonated in the United States and abroad.[63] The European Commission, for example, is currently considering a controversial proposal to include the "right to forget" in its data privacy laws.[64]

The concept of political obscurity builds this dialogue. Stopping far short of mandated digital forgetting, the call to respect citizens' right to political obscurity asks the state to remove itself from the role of facilitating online dissemination of information that reveals our political preferences.

B. Political Obscurity and the Court

The Supreme Court has not formally recognized a right to political obscurity. This is unsurprising. Since the founding of this nation until very recently, time and information inefficiencies safeguarded the political obscurity of the vast majority of Americans. But the Court has consistently policed the role of the state in disclosing political identity, affirming that the right to political privacy is firmly rooted in core First Amendment political self-determination and personal autonomy rights.

1. Political Affiliation—Cold War and *NAACP*

State-mandated political identity disclosure cases litter Supreme Court history, most predominantly during the Cold War Period, and in other periods of pronounced political strife.[65] Many such cases involved a prying state and the desire of citizens to avoid classification that could draw hostile reaction from the state and/or members of the public. Particularly during the Cold War, when state actors attempted to rout "subversive behavior," the Court played a central role in protecting against forced disclosure of political identity.[66]

In addition to Cold War Era political privacy cases, the Court's right of association jurisprudence confirms the constitutional commitment to protecting against state-facilitated disclosure of one's political preferences.[67] The seminal associational

62. *Id.* at 135.

63. Congressman Ed Markey of Massachusetts has authored a bill, for example, that would require erasure of online records on children. Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011).

64. Meg Leta Ambrose & Jef Ausloos, The Right to Be Forgotten Across the Pond 8–9 (Sept. 21, 2012) (unpublished paper), *available at* http://ssrn.com/abstract=2032325 (discussing key provisions in the European Commission's proposal for a regulation regarding the processing of personal data and the free movement of such data).

65. For a thorough review of disclosure cases during the Cold War, see Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 7–10 (1991).

66. *See, e.g.*, Sweezy v. New Hampshire, 354 U.S. 234, 254–55 (1957) (overturning on due process grounds contempt conviction for refusal to answer questions regarding petitioner's political beliefs); United States v. Rumely, 345 U.S. 41,42 (1953) (Douglas, J., concurring) ("If the lady from Toledo can be required to disclose what she read yesterday and what she will read tomorrow, fear will take the place of freedom in the libraries, bookstores, and homes of the land."); Thomas v. Collins, 323 U.S. 516, 534 (1945) (finding the First Amendment protects the right "fully and freely to discuss and be informed concerning this choice, privately or in public assembly").

67. *See* William O. Douglas, *The Right of Association*, 63 COLUM. L. REV. 1361, 1372–83 (1963) (detailing the threat to the right of association protected by the First Amendment posed by legislative

rights case *NAACP* provides an example.[68] In *NAACP*, the Attorney General of Alabama brought suit against the civil rights group for failing to comply with a state statute requiring "foreign" (i.e., non-Alabamian) corporations to register with the Secretary of State.[69] During litigation, the State moved for production of a large number of NAACP documents, "including bank statements, leases, deeds, and records containing the names and addresses of all Alabama 'members' and 'agents' of the Association."[70] The NAACP eventually turned over all of the documents except for its membership lists and subsequently suffered a contempt judgment for failing to comply fully with the production order.[71] The NAACP's chief argument was that compelled disclosure of the membership lists violated the group and its members' right of free association.[72]

The Court found in favor of the NAACP and the political privacy interests of current and potential NAACP members (recognizing that without ensuring the "collective privacy" of the group, the NAACP would be unable to draw new members).[73] The Court understood the crucial link between protecting privacy in political belief and ensuring public political participation.[74] *NAACP* therefore strikes at political obscurity's core: it cements the right of individuals to define and control zones of political activity in order to ensure such political activity takes place. Implicit in right of association cases is political obscurity: the recognition that individuals must be free to define the spheres in which their political identity travels.

2. Political Anonymity—*McIntyre*

In *McIntyre v. Ohio Elections Commission*,[75] the Court reviewed the constitutionality of an Ohio statute requiring citizens distributing political literature to include their names, ultimately protecting Mrs. McIntyre's right to distribute her

investigative committees).

68. *See* Doe v. Reed, 130 S. Ct. 2811 (2010) (using the standard from *NAACP*); Ashutosh Bhagwat, *Associational Speech*, 120 YALE L.J. 978, 985–86 (2011) ("[T]he key [step in associational privacy rights] from the point of view of modern law, was the Court's 1958 decision in *NAACP v. Alabama*."); Stephen Clark, *Judicially Straight?* Boy Scouts v. Dale *and the Missing Scalia Dissent*, 76 S. CAL. L. REV. 521, 542 (2003) (describing *NAACP v. Alabama* as one of the "foundational cases" in associational privacy); Edward J. Eberle, *The Right to Information Self-Determination*, 2001 UTAH L. REV. 965, 979 (2001) ("NAACP v. Alabama, decided amidst the civil rights struggle, is the leading case on group privacy and associational rights.").

69. *NAACP*, 357 U.S. at 451–53; *accord* Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87 (1982) (challenging the constitutionality of the disclosure provisions in the "Ohio Campaign Expense Reporting Law"); Bates v. Little Rock, 361 U.S. 516 (1960) (challenging an Arkansas municipality ordinance demanding a local branch of the NAACP to give city officials a list of their members).

70. *NAACP*, 357 U.S. at 453.

71. *Id*. at 453–54.

72. *Id.* at 458–59.

73. *See id.* at 462–63 ("[C]ompelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.").

74. *Id.* at 462.

75. 514 U.S. 334 (1995).

pamphlets anonymously. *McIntyre* is therefore widely cited for its pronouncements on anonymity.[76] But the case also has a lot to say about political obscurity. First, although Mrs. McIntyre resisted the requirement that she put her name on all of her handbills, she put her name on many and indeed distributed many handbills herself in plain view of others.[77] *McIntyre* is therefore very much about the scope of information release—specifically, Mrs. McIntyre's ability to control how many people knew she was the author of her pamphlet.[78] What bothered Mrs. McIntyre was the State of Ohio forcing her to reveal her identity on a broader scale than she preferred.[79] In that sense, the right to political obscurity is central in the case.

One feature that unites Cold War Era political privacy cases and *McIntyre* is the absence of technology as a central element of the case. These cases exist in an ink-and-paper world. Looming databases, computer-aided information sharing, and the Internet are largely irrelevant to the cases that provide the basis for political privacy rights in this country.[80] The Court has addressed technology-enhanced disclosure in several nonpolitical contexts. Although there have been glimmers of recognition that technology dramatically alters the disclosure balance, *Reporters Committee* being a prime example,[81] most cases have held that amplified disclosure through placement on a computer database or on the Internet does not materially impact the outcome.[82]

3. Location Obscurity—*Jones*

One case from the 2012 Supreme Court Term suggests an evolving understanding of the value of obscurity as it relates to technological advance. A concurring opinion in

76. *See, e.g.*, Justice for All v. Faulkner, 410 F.3d 760, 764 (5th Cir. 2005).

77. *McIntyre*, 514 U.S. at 337 ("Some of the handbills identified [Mrs. McIntyre] as the author; others merely purported to express the views of 'CONCERNED PARENTS AND TAX PAYERS.' Except for the help provided by her son and a friend, who placed some of the leaflets on car windshields in the school parking lot, Mrs. McIntyre acted independently."). Justice Scalia uses Mrs. McIntyre's signing her name to a subset of her handbills as evidence that she did not fear *NAACP*-style threats or harassment, entirely missing the more subtle point that Mrs. McIntyre sought the ability to control the scope of disclosure. *Id*. at 380 (Scalia, J., dissenting).

78. *See id.* at 342.

79. *See id.* at 355 (distinguishing mandatory disclosure of political expenditures from compelled self-identification on all election-related writings).

80. *Doe v. Reed*, however, is an exception. See *infra* notes 99–109 and accompanying text for a discussion of *Doe v. Reed*.

81. *See* Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan, J. concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.").

82. *See, e.g.*, *id.* at 600 (majority) ("We are persuaded . . . that the New York program [creating a computer database of individuals prescribed Schedule II opiates by their doctor] does not, on its face, pose a sufficiently grievous threat to either interest to establish a constitutional violation."); Nat'l Aeronautics & Space Admin. v. Nelson, 131 S. Ct. 746, 763–64 (2011) (refusing plaintiffs' claim that databasing of information gleaned from government background checks would subject employees to possible disclosure of sensitive personal information); Connecticut Dept. of Pub. Safety v. Doe, 538 U.S. 1, 6–7 (2003) ("Mere injury to reputation [due to posting of sex offenders' personal information on an online sex offender registry] . . . does not constitute the deprivation of a liberty interest.").

the Fourth Amendment case *United States v. Jones*[83] (involving twenty-four-hour GPS surveillance) suggested that members of the Court may be increasingly sensitive to the issue of technology-enhanced disclosure of personal information.[84] Wrote Justice Sotomayor:

> I would take [the] attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.[85]

Sotomayor went on: "[m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[86] Though she did not use the word, Sotomayor is arguing for a right to obscurity. Sotomayor recognizes that while we may share information about ourselves in limited spheres—walking down the street, a limited group of others may see us pass and take note of our movements—technology-enhanced disclosure fundamentally changes the equation.[87] Similarly, when we disclose information about our political preferences in limited spheres of our choosing, the state's use of technologies that take that choice away and amplify disclosure beyond what we intend violates the right to political obscurity.

With these musings in mind, the next Part focuses on the Court's handling of the right to prevent disclosure of political identity in the petition context up to and including *Reed*. The Court's treatment of political obscurity in petition cases reveals a puzzle: its importance is recognized in pretechnology cases but is oddly undervalued in the technology-driven case of *Reed*.

C. Political Obscurity and Petitions

The first cases to discuss one's ability to control information about political preferences in petitioning centered not around the privacy interests of petition signers, but around those of petition circulators. In *Buckley v. American Constitutional Law Foundation, Inc.* (ACLF),[88] the State of Colorado placed restrictions on petition circulators, including the requirement that each wear a name badge bearing their true

83. 132 S. Ct. 945 (2012).

84. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'").

85. *Id*. at 956.

86. *Id*. at 957.

87. *See id.* at 954–57 (drawing a distinction between societal expectations of disclosure of public movements and technology-enhanced surveillance by the government).

88. 525 U.S. 182 (1999). Throughout this Article, I will refer to *Buckley v. American Constitutional Law Foundation, Inc.* as ACLF as it is commonly known throughout legal scholarship. I will, however, continue to cite the case using the title as is appears in the *United States Reports*.

name.[89] The plaintiffs argued that the requirement dramatically reduced the ranks of those willing to circulate petitions.[90] Explained a veteran political organizer testifying in the case, "[t]he badge requirement . . . 'very definitely limited the number of people willing to work for us and the degree to which those who were willing to work would go out in public.'"[91]

Like *McIntyre*, ACLF is most often cited as an anonymity case.[92] Forcing circulators to wear name badges felt the same as requiring Mrs. McIntyre to affix her name to her pamphlets a few years earlier—a plain-vanilla matter of forced identity disclosure. But ACLF, like *McIntyre*, is a strange brand of anonymity. The circulators, after all, were not masked. Anyone who recognized the petition circulators would learn of their political preferences on the subject of the petition being circulated. By not wearing name badges, circulators maintained a desired degree of political obscurity. Requiring circulators to wear name badges forced them to expand the scope of disclosure of their political preferences (and thanks to the registration requirement, that scope expansion included exposure to state cataloging).

The Court's analysis in ACLF is somewhat scattered. At points, the Court noted concern for *NAACP*-style retaliation and harassment.[93] But in the end, the Court did not require proof of potential or actual retaliation or harassment to reach its conclusion.[94] The decision comes down to the Court's concern for maintaining high levels of political participation.[95] Wrote the Court, "Colorado's current badge requirement discourages participation in the petition circulation process by forcing name identification without sufficient cause."[96] Forcing name identification, in other words, dilutes political obscurity to the detriment of democratic functioning.

89. *Am. Constitutional Law Found.*, 525 U.S. at 186.

90. *Id.* at 195–96.

91. *Id*. at 198.

92. *See, e.g.*, Gayle Horn, *Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines*, 60 N.Y.U. ANN. SURV. AM. L. 735, 767 (2005) ("In *Buckley v. American Constitutional Law Foundation*, the Supreme Court extended this right to anonymity to the circulation of petitions . . . ." (footnote omitted)); Sharon K. Sandeen, *In for a Calf Is not Always in for a Cow: An Analysis of the Constitutional Right of Anonymity as Applied to Anonymous E-Commerce*, 29 HASTINGS CONST. L.Q. 527, 571 (2002) ("In *Buckley v. American Constitutional Law Foundation*, the Supreme Court again considered the right of anonymity in the context of political speech."); Darryl R. Wold, *Tell Us Who You Are - Maybe: Speaker Disclaimers After* Citizens United, 16 NEXUS: CHAP. J.L. & POL'Y 171, 186 (2011) ("The Court again visited the issue of anonymity in political speech in *Buckley v. American Constitutional Law Foundation* (*'ACLF'*).").

93. For example, the Court cited testimony indicating the "reluctance of potential circulators to face the recrimination and retaliation that bearers of petitions on 'volatile' issues sometimes encounter: '[W]ith their name on a badge, it makes them afraid.'" *Am. Constitutional Law Found.*, 525 U.S. at 198 (alteration in original).

94. *Id.* at 200.

95. *Id.* at 198–200.

96. *Id.* at 200; *see also* Watchtower Bible & Tract Soc'y of N.Y. v. Vill. of Stratton, 536 U.S. 150 (2002) (holding unconstitutional a state statute requiring door-to-door canvassers obtain a license from the town). *Watchtower Bible* did not concern a name badge requirement, but the Court echoed ACLF's concern for contained political identity. "In the Village, strangers to the resident certainly maintain their anonymity, and the ordinance may preclude such persons from canvassing for unpopular causes." *Watchtower Bible*, 536 U.S. at 167.

After *McIntyre* and ACLF, some believed the Court would continue to prefer individual political privacy rights over disclosure.[97] Boy, were they wrong![98] In the petition context, *Doe v. Reed* heralded what seemed to be an about-face. The *Reed* Court (and the court below in the as-applied remand) ignored the value of political obscurity. The Court, in large part due to the plaintiffs' litigation strategy,[99] rested its decision on the question of retaliation.[100] If the State of Washington released signers' names, would signers then be exposed to *NAACP*-style threats and retaliation? For reasons discussed in the introduction, the answer was a resounding no.[101]

A second ground to deny the plaintiffs' plea for privacy in petition signing was the public nature of the act itself. Justice Scalia's concurrence hammered this point home.[102] Consistent with his prior writing on the subject,[103] Scalia rejected outright that a right to privacy even exists in petitioning, which he argued is at its core a legislative act.[104] Scalia meticulously documented the history of petitioning in public, from open town hall meetings in colonial New England, to reading petitions aloud in Congress in 1790, to the roots of the progressive direct democracy movement in the early 1900s.[105] In the history of this country, and indeed for centuries before in European antecedents, the right to petition the government never included the right to petition privately.[106] Scalia therefore finds the idea that a privacy right might attach to the public act of petitioning preposterous.[107] For Scalia, political obscurity does not exist. You are either fully in or fully out.[108]

What Scalia and the majority missed, however, is that history is largely irrelevant

97. McGeveran, *supra* note 28, at 859–60.

98. McGeveran recently noted that he previously had tracked a trend of what he believed might be "a more capacious understanding of the interests in anonymity when ordinary individuals engage in politically-related speech." *Id.* at 859. By 2011, after *Citizens United* and *Doe v. Reed*, McGeveran wonderfully laments, "[b]oy was I wrong." *Id.* at 860.

99. *See* Doe v. Reed, 130 S. Ct. 2811, 2814 (2010) ("The problem for plaintiffs is that their argument rests almost entirely on the specific harm that would attend the disclosure of information on the R–71 petition.").

100. *Id.* at 2817–20.

101. *Id.* at 2821. ("Faced with the State's unrebutted arguments that only modest burdens attend the disclosure of a typical petition, we must reject plaintiffs' broad challenge to the PRA."). See *supra* Part II.C for a discussion of the *Reed* Court's treatment of the speculative harm to plaintiffs.

102. *See id.* at 2833–36 (2010) (Scalia, J., concurring) (discussing the history of public voting and legislating).

103. *E.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 371–85 (1995) (Scalia, J., dissenting).

104. *Reed*, 130 S. Ct. at 2832–33 (Scalia, J., concurring) ("Our Nation's longstanding traditions of legislating . . . in public refute the claim that the First Amendment accords a right to anonymity in the performance of an act with governmental effect.").

105. *Id.* at 2834. (citing STEVEN L. PIOTT, GIVING VOTERS A VOICE 1-3, 5 (2003)). Scalia also reviews the history of a cousin of petitioning: casting of ballots, which until later in U.S. history, Scalia notes, was considered a public act. *Id.* at 2834–36.

106. See *infra* notes 148–52 and accompanying text for discussion of the history of petitioning in the United States.

107. *See Reed*, 130 S. Ct. at 2834–36 (Scalia, J., concurring) (chronicling the history of public disclosure in federal governmental functions).

108. *See id.* at 2836–37 (concluding that the Constitution does not impose any secrecy requirement upon the states).

to the true harm suffered in *Reed*. Technological threats to political obscurity *not present in the past* are at the core of the case.[109] Pre-Internet, those who signed petitions might have expected that the petition circulator or others signing the same page of the petition might see their name. Signers would expect that government officials might verify the validity of their signature. The possibility vaguely loomed that concerned citizens might pore over the pages of paper signatures looking for fraud. But, due to the paper-based information architecture, petition signers of old had no expectation that the government would affirmatively publicize their signature in a permanent, searchable format (for the simple reason that, until recently, no means to do so were available). Petition signers could rely on the political obscurity that exists in a paper-based information architecture. Today, however, petition signing is experiencing a fundamental shift. The Section that follows examines how profound the shift is.

III. THE MODERN THREAT TO POLITICAL OBSCURITY

We now live in a society with a perfect digital memory; the Internet does not forget.[110] Petition signers in *Reed* tried to convey this, expressing fear of "economic reprisals," not just in the form of firing from their current job or boycott of businesses in real time.[111] In a world without political obscurity, repercussions loom indefinitely. What is the real cost of signing petitions when doing so potentially creates a permanent record of one's political beliefs in the everlasting memory of the Internet?

A. The Modern Political Data Infrastructure

Over the course of a digital citizen's lifetime, a variety of organizations compile an increasingly broad spectrum of data about him.[112] Information about spending and saving habits, consumer product preferences, home ownership, and a wide swath of other forms of data, are regularly compiled into dossiers used for a wide variety of purposes.[113] An entire industry has arisen devoted to culling, tracking and selling huge

109. Alito's concurrence emphasized the Internet's potential for making personal information available to be used for harassment. *Id*. at 2825 (Alito, J., concurring). Alito noted the *NAACP* link between privacy and political participation, worrying that compelled disclosure of names on petitions could "burden the ability to speak," and thereby "seriously infringe on privacy of association and belief guaranteed by the First Amendment." *Id*. at 2822 (quoting Citizens United v. Fed. Election Comm'n, 130 S. Ct. 876, 914 (2010); Buckley v. Valeo, 424 U.S. 1, 64 (1976)). Alito rejected the facial challenge, but suggested these rights could well be vindicated through an as-applied challenge. *See id.* at 2824 (finding "courts should be generous in granting an as-applied relief in this context"). Although he joined the majority, Alito worried that invading privacy interests of petition signers might, "chill the willingness of voters to sign" a referendum petition (and thus the circulator's ability to collect the necessary number of signatures). *Id*. at 2822.

110. *See generally* MAYER-SCHÖNBERGER, *supra* note 61 (discussing the paradigmatic shift, caused by information technology, from forgetfulness to perfect memory).

111. *See* Brief for Petitioner, *supra* note 7, at 10–11 (outlining the evidence of intimidation against petitioners).

112. The "digital person," does not just refer to individuals who spend time online, but increasingly even those who do not and yet still find their real world activities catalogued by digital information gatherers. *See generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) (discussing how various organizations monitor our habits on the Internet and the threat to our privacy as a result).

113. Daniel Solove is one of the first and most prolific writers to identify and dissect the impact of this

amounts of information about people from individual consumer preferences, to Internet browsing histories, to location data.[114] Some studies suggest that consumers do not much care when companies track their preferences for marketing purposes.[115] Others indicate that perhaps consumers are starting to care.[116]

But the dramatic increase in *political* data aggregation practices in the past twenty years suggests that political privacy norms—namely, that citizens maintain relative control over the flow of information about their political preferences—are changing fast.[117] Data that reveals our political preferences and activities has become a valuable commodity for a variety of end users including, but not limited to, those seeking to sway political outcomes through a variety of voter targeting efforts.[118]

Before computers, state parties and individual campaigns developed relatively crude databanks on voters and campaign donors collected through voter phone calls and door-to-door canvassing.[119] This information might include the voter's candidate

trend. *See id.* at 16–26 (discussing how data collection captures almost all Internet activity but is difficult for the average Internet user to appreciate). Solove explains:

> As we live more of our lives on the Internet, we are creating a permanent record of unparalleled pervasiveness and depth. Indeed, almost everything on the Internet is being archived. One company has even been systematically sweeping up all the data from the Internet and storing it in a vast electronic warehouse. Our online personas—captured, for instance, in our web pages and online postings—are swept up as well. We are accustomed to information on the web quickly flickering in and out of existence, presenting the illusion that it is ephemeral. But little on the Internet disappears or is forgotten, even when we delete or change the information. The amount of personal information archived will only escalate as our lives are increasingly digitized into the electric world of cyberspace.

Id. at 26. *See also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 163–65 (2000) (discussing the efforts of advertisers to gather information from Internet users); Berkman Center for Internet & Society, *Joel R. Reidenberg on Transparent Citizens and the Rule of Law*, HARVARD UNIVERSITY (Feb. 1, 2010), http://cyber.law.harvard.edu/interactive/events/lawlab /2010/02/reidenberg (exploring the erosion of the boundary between public and private information on the Internet).

114. *See* SOLOVE, *supra* note 112, at 17–22 (describing the development of the direct marketing and database industries).

115. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 19, 2012, (Magazine), at 30 (describing how retailers create predictive models from data on consumer habits unbeknownst to the consumer).

116. One study found that sixty-six percent of Americans say that they do not want their information used to target consumer products to them. Joseph Turow et al., Americans Reject Tailored Advertising and Three Activities that Enable It 3 (Sept. 29, 2009) (unpublished paper), *available at* http://ssrn.com/abstract=1478214. When participants in the study were told how companies would target them (through their activity on the website, through activity on other websites, and through their offline activity), between seventy-three and eighty-six percent said that they would not want such advertising. *Id.*

117. *See* Daniel Kreiss & Philip N. Howard, *New Challenges to Political Privacy: Lessons from the First U.S. Presidential Race in the Web 2.0 Era*, 4 INT'L J. OF COMM. 1032, 1035 (2010) (discussing the diminution of traditional political privacy as political participants share personal information).

118. *See* SOLOVE, *supra* note 112, at 20 (describing companies that specialize in compiling demographic and voting data); *cf.* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1406–09 (2001) (explaining the historical rise in targeted marketing).

119. *See* Philip N. Howard & Daniel Kreiss, *Political Parties and Voter Privacy: Australia*, *Canada, the United Kingdom, and United States in Comparative Perspective*, 15 FIRST MONDAY (Dec. 6, 2010), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article /view/2975/2627 (warning about the harmful

preferences, top issues of concern, and the voter's activist history (such as whether the voter has volunteered as a precinct captain or whether the voter had served as a poll worker). In many states, a basic building block of campaign voter data files came from the state in the form of state voter registration and voter history data.[120] But these early efforts at sourcing political data in public records and campaign outreach efforts are quaint compared to the newest iterations of the practice. As the information revolution has unfolded, political data mining efforts have become extraordinarily sophisticated.[121]

Beginning in the 1980s, the Republican Party began using consumer data, particularly commercial data such as credit card records and magazine subscription lists to target voters and identify prospective donors.[122] After the 2004 election, the Democratic Party began to outsource political data mining to private companies to streamline, update, and expand voter file data.[123] In 2008, the Democratic Party and the Obama campaign, aided by a long, multistate Democratic primary battle, helped the Democrats build a centralized voter file dubbed the Voter Activation Network.[124] Senator Al Franken's win in Minnesota in 2008 is widely credited to Democrats' sophisticated political data aggregation effort.[125] In that recount, election lawyers used the Democrats' voter data profiling to predict ballot outcomes as a means of honing its

effects of increased data mining in the political context); Kreiss & Howard, *supra* note 117, at 1035 (explaining how "powerful advances in computing during the 1970s made data management skills and raw datasets stored on mainframes newly bankable assets for consultants and parties"); Daniel Kreiss, *Yes We Can (Profile You): A Brief Primer on Campaigns and Political Data*, 64 STAN. L. REV. ONLINE 70, 71 (2012) (discussing "the history of political data, focusing on the recent proliferation in voter data and development of new voter modeling techniques").

120. Twenty-nine states currently outlaw the commercial use of voter registration lists. This includes allowing third parties to use the lists for commercial reasons. Kim Alexander & Keith Mills, *Voter Privacy in the Digital Age*, CAL. VOTER FOUND. (last updated Jan. 23, 2012), http://www.calvoter.org/issues/votprivacy/pub/voterprivacy/findings.html. Twenty-two states have no restraints on use of voter data and allow unrestricted use of voter registration files. *Id*.

121. Kreiss & Howard, *supra* note 117, at 1035–36 (noting that while the Democratic Party initially lagged behind in these efforts, it has pioneered recent efforts to collect data from supporters since 2008).

122. *Id*.

123. *Id.* at 1036.

124. *Id.*; *cf.* Noah Rothman, *Republican National Committee to Outsource Voter File*, CAMPAIGNS & ELECTIONS, May 23, 2011, http://www.campaignsandelections.com/campaign-insider/Republican-National-Committee-to-Outsource-Voter-File (discussing the Republican National Convention's plan to share its voter file with independent groups). According to Kreiss & Howard, the Obama campaign

> continually analyzed user behavior on its Web site and made minor adjustments in design and content that increased the percentage of citizens who signed up for its e-mail list and donated money. Together, the electoral databases maintained by the Democratic National Committee and by the private firm Catalist, in conjunction with a vast array of online behavioral and relational data collected from use of the campaign's website and third-party social media sites such as Facebook, provided the Obama campaign with data on more than 250 million Americans.

Kreiss & Howard, *supra* note 117, at 1033.

125. JAY WEINER, THIS IS NOT FLORIDA: HOW AL FRANKEN WON THE MINNESOTA RECOUNT 133 (2010) ("More than once, voting officials and Coleman reps witnessed Franken lawyers check with staff members—'computer geeks' . . . —who sorted through voter data information on their laptops. In a few cases, the staffer with the computer gave a thumbs-up or thumbs-down to the Franken lawyer, and a decision was made.").

successful litigation strategy.[126]

Since then, companies have proliferated, advertising the ability to identify and target voters for campaign donations, get out the vote efforts, and customized mailing (and emailing and social network) campaigns.[127] Others, through increasingly sophisticated software, are marketing the ability to identify patterns of voter behavior and taste believed predictive of voter decision making.[128] Whether they are political data mining outfits or "digital political advertising" firms, the basic idea is that sophisticated data profiling of individual voters—from cars they drive to websites they visit to the traffic tickets they incur—allows campaigns not only to identify potential supporters, but to customize the message to that individual voters receive based on their data profile.[129] Companies like CampaignGrid on the conservative side and DSPolitical and Precision Network on the liberal side promise to make every campaign dollar go towards hitting the right voters with the right message.[130] Aggressive political data efforts marked the 2008 campaign on both sides, with very little if any oversight on collection practices and use of collected voter data.[131]

For the most part, voters remain clueless about the extent and sophistication of political data collection and use.[132] Just before Mitt Romney in 2012 announced his running mate, CNN broadcast that anyone who downloaded the Romney campaign's "mobile app" would receive word of the running mate pick in advance.[133] What most did not realize, however, is that downloading the mobile app created a treasure trove of

126. *Id*.

127. Kreiss & Howard, *supra* note 117, at 1036–39.

128. *See, e.g.*, SOLOVE, *supra* note 112, at 20 (discussing software that implements advanced methods for predicting how individuals will vote).

129. Colin Delany, *Voter File Digital Ad Targeting: Reality vs. Hype*, CAMPAIGNS & ELECTIONS, July/Aug. 2012, at 20.

130. *Id.* Daniel Solove, for example, described how a political data marketer called Aristotle maintains a "Fat Cat" list it sells to candidates with the following pitch: "Hit your opponent in the Wallet! Using Fat Cats, you can ferret out your adversary's contributors and slam them with a mail piece explaining why they shouldn't donate money to the other side." SOLOVE, *supra* note 112, at 20. GeoVoter, Solove notes, "combines about 5,000 categories of information about a voter to calculate how that individual will vote." *Id.*; *see also* McGeveran, *supra* note 28, at 873–75 (expressing concerns for diminished privacy rights as a result of new digital dossiers).

131. *See* Kreiss & Howard, *supra* note 117, at 1041–42 (noting the lack of transparency around political campaign use of data and lack of regulation, largely due to First Amendment free speech protections campaigns enjoy). Rampant inaccuracies in political data streams are starting to cause problems that are likely to increase in frequency. *Id.* at 1042. Problems associated with corrupted voter data are proliferating. *Id.* at 1042–43. During the 2012 election in Virginia, for example, an organization mailed voter registration forms with prepopulated and allegedly inaccurate voter data belonging to deceased individuals, pets, and non-citizens. Wesley P. Hester, *Romney Camp Asks Va. to Probe Voter Forms*, RICHMOND TIMES DISPATCH, July 25, 2012, at A1.

132. *See* Kreiss & Howard, *supra* note 117, at 1041 (finding that few citizens are aware of contemporary campaign practices because they are generally hidden from the public).

133. *Campaigns Debut Mobile Apps*, CNN (July 31, 2012, 8:34 AM), http://politicalticker.blogs.cnn.com/2012/07/31/campaigns-debut-mobile-apps/ ("Team Romney's app, called 'Mitt's VP,' will send a notification to users when the candidate is ready to announce his vice presidential selection. The campaign said the app would be the 'first official distribution channel' for the big reveal.").

data for the Romney campaign.[134] Explained one report on the privacy implications of mobile apps,

> Smartphones are often on and tethered to their user, transmitting rich data to the app developers. Users of mobile devices are vulnerable to privacy intrusion and abuse by numerous entities, app developers, analytic services and advertising networks. These entities could have access to sensitive information, including a user's location, contacts, identity, messages and photos. Without a privacy policy [which very few mobile apps include], what companies do with the personal data they collect is largely invisible to consumers.[135]

A final observation about political data mining relates specifically to petitioning. Unlike other data points such as the cereal one eats, one's age, or one's history of volunteering for political campaigns, petition data is particularly revealing. Other data points might lead campaigns and others to hypothesize about voting preferences through sophisticated algorithms and guesswork. The resulting predictions may pinpoint voter preferences exactly or be way off. Petition signing data, however, is far more fine-tuned and invasive of political obscurity. Like a ballot, it may reveal the core content of their political identity.[136]

Rampant political data mining creates a climate unlike anything democracy has known. Political obscurity is fast becoming a thing of the past—and without most voters realizing it. Current petition practices feed the data deluge collected on ordinary people's political preferences. This may be of great concern to some; others might shrug it off. The next Part reviews the pros and cons of diminishing political obscurity in petitioning.

B. Political Obscurity and Petitioning: Should We Care?

Growing empirical evidence suggests that waning political obscurity threatens petitioning.[137] In one study, researchers asked subjects how likely they were to sign a

134. *Id.*

135. Press Release, Cal. Dept. of Justice, Office of the Attorney General, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications, (Feb. 22, 2012). Joseph Lorenzo Hall recently pointed out the issue of campaigns collecting voter data through mobile apps in a post on the Election Law Listserv. Joseph Lorenzo Hall, *ELB News and Commentary* (July 31, 2012, 8:54 AM), http://department-lists.uci.edu/pipermail/law-election/2012-July/004332.html (responding to Richard Hasen's observation—that the Obama campaign uses the cell phone number Hasen provided to send campaign-related text messages—by explaining that a mobile app allows campaigns to collect far more information).

136. There are at least two reasons to step back from this statement. First, as discussed *infra* Part IV.A, many petition signers (in the case of nonofficial online petitions) do not use their real name. Still, this does not ensure that identity is not traceable. *See* Allesandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROCEEDINGS NAT'L ACAD. SCI. 10975, 10975 (2009) (describing the technological feasibility of combining bits of data to determine identity). Second, signing a petition does not always indicate political preference. For example, initiative petitions involve whether or not a particular issue should be put to voters; signers of such petitions may not be expressing a political preference other than a belief that voters should take it up at the next election.

137. La Raja, *supra* note 1, at 1 (arguing that decreasing anonymity has a chilling effect on political participation).

petition in support of a candidate or cause they believed in, even if that candidate or cause was unpopular with friends or coworkers.[138] Researchers then asked those respondents how likely they were to sign a petition that is posted publicly on the Web in support of a cause or candidate they believed in, but was unpopular with friends and coworkers.[139] When respondents were told that their signatures would appear on the Internet, their willingness to sign a petition dropped by 8.5%.[140] If people believe they have lost control over the scope of disclosure of their political preferences, they may become very wary of disclosing those preferences at all.[141]

Despite these trends, some might argue if some people decline to sign citing privacy concerns, these are minor casualties; the new data architecture aids the democracy by enhancing accountability.[142] We cannot have a deliberative democracy without citizens actively pronouncing their views and being accountable to those views.[143] The supporters of gay marriage in California, like those in Washington State,

138. *Id.* at 13.

139. *See id.* at Abstract. ("[Our] findings indicate that . . . people are less willing to sign a petition when they believe the petition will appear on the Internet. Important differences exist for women and cross-pressured citizens. The results imply that disclosure policies regarding . . . petition signers involve social costs that negatively affect political participation.").

140. *Id.* at 17.

141. It bears mention that data overexposure pollutes the petitioning process in other ways as well. In 2011, a group called Californians Against Identity Theft and Ballot Fraud aired radio advertisements warning California voters that signing petitions could expose them to identity theft. Torey Van Oot, *Californians Against Identity Theft Files as Campaign Committee*, SACRAMENTO BEE (Aug. 3, 2011, 12:43 PM), http://blogs.sacbee.com/capitolalertlatest/2011/08/californians-against-identity-theft-campaign-committee.html. The group warned that information from petitions could be used to perpetrate identity theft and that names on petitions have already been sent overseas for nefarious uses. Paul Jacob, *Crying Fire in a Crowded Democracy*, TOWNHALL (July 31, 2011), http://townhall.com/columnists/pauljacob/2011/07/31/crying_fire_in_a_crowded_democracy/page/full/. The group cited the rise of paid canvassers, often recruited among indigent populations, as further evidence that signatures are at risk. *See id*. (referencing a group member who called petition circulators "paid bounty hunters"). The group backed its claims with references to the lack of regulation of California official petition-signature gatherers. *Unions Targeted by Ballot Petitions Counter Campaigns*, GOERIE.COM (July 31, 2011, 7:23 AM), http://www.goerie.com/apps/pbcs.dll/article?AID=/20110731/NEWS07/307319898/-1/ETN. Most outside groups, including Common Cause, have expressed their belief that the ad was created to provoke fear and to keep Californians from signing petitions. Nikki Willoughby, *Intimidation Tactics in California*, COMMONBLOG (Aug. 1, 2011), http://www.commonblog.com/2011/08/01/intimidation-tactics-in-california/. Given the backing of labor unions, particularly the State Building and Construction Trades Council of California, some outsiders have suggested that the group's ads are targeted at potential pension reform referenda. *Unions Targeted by Ballot Petitions Counter Campaigns*, *supra*. The sponsors of the group, however, have defended its warnings as targeted to better regulate the signature-gathering industry within California, citing incidents of deceptive practices by paid canvassers. *Id*. A similar incident occurred in Michigan. *The MI GOP Freakout Cont'd: Robocalls Warn Against Identity Theft*, Daily Kos (Aug. 11, 2011, 5:15 AM), http://www.dailykos.com/story/2011/08/19/1008542/-The-MI-GOP-freakout-cont-d-Robocalls-warn-against-identity-theft-from-signing-petitions-AUDIO-link.

142. *See* DENNIS BAILEY, THE OPEN SOCIETY PARADOX: WHY THE 21ST CENTURY CALLS FOR MORE OPENNESS–NOT LESS 201 (2004) ("Life in a global village is likely to impact our lives significantly as events normally hidden from the public eye become transparent, forcing people to take more accountability for their actions.").

143. *See, e.g.*, Doe v. Reed, 130 S. Ct. 2811, 2837 (Scalia, J., concurring) (discussing the need for people to "stand up in public" for their views in order for democracy to function).

wanted to post petition signers' names and addresses with Google map directions precisely because they hoped to encourage those who stood for gay marriage to challenge those who opposed it.[144] This is how America works. We debate. We confront. Too much political obscurity makes it impossible for such confrontation and debate to take place.[145] Those "tough conversations," the argument goes, are valuable to democracy.

What this position overlooks, however, is that without some measure of political obscurity we will have far fewer individuals to hold to account. To the extent that "outing" petition signers drives *would-be* petition signers away from petition clipboards, we may never know who supports or opposes what in a post-political obscurity world. We will still know the political preferences of those who stand very publicly behind their convictions. Indeed, there will always be vocal and public supporters of causes who court, and even enjoy, broad and lasting political exposure. But, what if the vast majority of citizens who value political obscurity simply withdraw? Reduced participation in petitioning may well have negative impact on other forms of political participation, such as contributing to political campaigns and even voting.[146]

A second criticism of the idea that fading political obscurity will erode participation in petitioning is that far from dampening participation, technology *facilitates* political participation on a scale never before imagined.[147] Anyone who has picked up the newspaper in the last year knows that online petitioning efforts have Change.org'ed the world. Perhaps the general population does not value political obscurity, as evidenced by the millions who seem undeterred by threats to privacy online petitioning may present.

To assess these claims, the following Section examines the trends of the two dominant forms of modern petitioning: official and popular petitioning. Section IV will examine the nuts and bolts of modern petition signature collection and processing with particular attention to the fate of political obscurity in each.

IV. MODERN PETITIONING

Petitioning in the modern day is in many ways thriving, meeting if not exceeding the Founders' expectations for public participatory democracy.[148] Petitioning in the United States takes two primary forms: "official" petitioning and "popular" petitioning.

144. Marder, *supra* note 34, at 450.

145. *See, e.g.*, *Reed*, 130 S. Ct. at 2837 (Scalia, J., concurring) ("Requiring people to stand up in public for their political acts fosters civic courage, without which democracy is doomed.").

146. *Cf.* Janine A. Parry, et al., *The Impact of Petition Signing on Voter Turnout*, 34 POLIT. BEHAV. 117, 132 (2012) (establishing through empirical study that petition-signing significantly enhances voter turnout, particularly among irregular voters.)

147. *See* La Raja, *supra* note 1, at 7 (highlighting research on the impact of "the Internet on politics").

148. Despite the proliferation and popularity of online popular petition sites in the last few years, pre-Internet petitioning in the preceding several decades witnessed a steep decline. Using data from Roper Political and Social Trends Survey (1973-1994), Robert Putnam describes the steep drop in political participation in this country generally, and petition signing specifically, in his 2000 book on U.S. political (in)activism. ROBERT D. PUTNAM, BOWLING ALONE 30–46 (2000).

Here, official petitioning refers to those instances in which the state requires petitioning as part of a legislative, judicial, or administrative process. A common example of official petitioning is a state's requirements for gathering a specified number of signatures to place a candidate on the ballot.[149]

Official petitioning also includes petitions circulated in support of direct democracy—the process of citizen legislating that enables voters to pass statutes and constitutional amendments via the ballot box.[150] Currently, about half of U.S. states have adopted some form of direct democracy.[151] Thus in many states official petitioning takes on an important role in the legislative process.[152]

Popular petitioning, by contrast, refers to spontaneous petitioning activities by members of the public to arouse support for a particular cause or call for specific action.[153] Popular petitioning has played a central role in political participation throughout U.S. history, particularly in moments of political and social upheaval.[154] Popular petitions, as described here, carry no legal effect; they seek to inform and alert decision makers who must then recognize and perhaps contend with a potentially sizable group.[155]

Popular petitioning and official petitioning serve separate functions and are

149. *See* Leonard P. Stark, *You Gotta Be on It to Be in It: State Ballot Access Laws and Presidential Primaries*, 5 GEO. MASON L. REV. 137, 140–41 (1997) ("Most states require candidates seeking a place on the ballot to gather petitions signed by registered members of the candidate's party. The number of required signatures varies from 500 statewide to more than 1000 in each of a state's congressional districts.").

150. John Gildersleeve, *Editing Direct Democracy: Does Limiting The Subject Matter of Ballot Initiatives Offend the First Amendment?*, 107 COLUM. L. REV. 1437, 1438–39 (2007). Direct democracy takes two main forms: initiatives (mechanisms that allows voters to propose a statute or state constitutional amendment first by gathering a requisite number of petition signatures to place the measure on the ballot) and referendums (mechanisms by which voters may challenge a measure enacted by a state legislature, again triggered by a minimum petition signature requirement). RICHARD J. ELLIS, DEMOCRATIC DELUSIONS: THE INITIATIVE PROCESS IN AMERICA 3–4 (2002). Direct democracy first arose during the Progressive Movement in the late 1800s when citizens began calling on direct popular input to combat perceived legislative practices. *Id.* at 26. Public opposition to industry-controlled state legislatures gave rise to a form of direct democracy, modeled on a democratic form in Switzerland, allowing citizens to vote directly on legislative matters. *Id.* at 28. For a review of the history of Swiss direct democracy, see PHILIP L. DUBOIS & FLOYD FEENEY, LAWMAKING BY INITIATIVE: ISSUES, OPTIONS AND COMPARISONS 46–70 (1998).

151. ELLIS, *supra* note 150, at 39.

152. Justice Scalia saw this aspect of official petitioning—its role in the legislative process—as determinative. For Scalia, no privacy interests can attach to public legislative acts. Doe v. Reed, 130 S. Ct. 2811, 2832 (2010) (Scalia, J., concurring); *see also* Chesa Boudin, Note, *Publius and the Petition:* Doe v. Reed *and the History of Anonymous Speech*, 120 YALE L. J. 2140, 2142 (2011) (arguing that petition signatures in referendums are solely legislative acts and should not be considered speech at all).

153. Stephen A. Higginson, *A Short History of the Right to Petition Government for the Redress of Grievance*, 96 YALE L.J. 142, 153–54 (1986) (discussing various local uses of petitions by eighteenth-century colonists, including the following: (1) petitions to obtain public funding for programs to care for the sick, insane, and orphans; (2) petitions to voice the grievances of unrepresented groups, such as women and slaves; and (3) petitions to modify legislation concerning agricultural and commercial developments).

154. For a detailed review of the role of petitioning in the United States, see generally Higginson, *supra* note 153, and Anita Hodgkiss, *Petitioning and the Empowerment Theory of Practice*, 96 YALE L. J. 569, 585 (1987).

155. *See* Higginson, *supra* note 153, at 156 (explaining that while citizens cannot bind Congress, the First Amendment maintains that citizens' petitions would be heard and considered).

carried out through distinctly different processes. The following Part starts with popular petitioning, offering a look at the basic forces in play and the fate of political obscurity in popular petition movements.

A. Modern Popular Petitioning

The Internet enables organizations to use online petition platforms to gauge public opinion and rally the public behind a cause quickly and virtually without cost. Building on this capacity, popular online petitioning platforms on which citizens (and noncitizens) can generate and sign online popular petitions are proliferating. [156] Topics range from: putting an immediate end to animal-tested cosmetics, abandoning the penny, requests to personally obtain medical marijuana, to withdrawing troops from Afghanistan.[157] Online popular petitioning is not necessarily directed at government; often such efforts are meant to sway private sector behavior.[158]

Nicholas Kristof documented the power of the online popular petition in a *New York Times* column.[159] Kristof described how a group of fourth graders created a petition at Change.org to protest the lack of environmental focus on the Universal Studios website promoting its film *The Lorax*.[160] According to the column, the petition gathered over fifty-seven thousand signatures and the studio promptly changed its website to include the environmental message the students had petitioned to add.[161] Countless examples suggest that the online petitioning platform has the power to create real results; it is a platform on which even a fourth-grade classroom can make change happen.

But harnessing consumer power is not the last word in online petitioning. Online popular petitioning has become a huge force in the political realm as well. The response to the proposed federal Stop Online Piracy Act (SOPA) in 2011 provides a good example. It featured an effort by Google, in which reportedly over seven million Americans petitioned Congress.[162] Importantly, signers who took the time to find out

156. Examples of popular U.S. online petitioning sites include Change.org, Care2, and iPetitions. *See About*, CHANGE.ORG, http://www.change.org/about (last visited Feb. 25, 2013) (describing Change.org as "world's largest petition platform, empowering people everywhere to create the change they want to see"); *Start Your Petition*, CARE2, http://www.thepetitionsite.com/create.html (last visited Feb. 25, 2013) (proclaiming Care2 as the "#1 petition site in the world,"); *About Us*, IPETITIONS, http://www.ipetitions.com/about (last visited Feb. 25, 2013) (providing that "the power of the internet [is] to transform society and [iPetitions] places it in the hands of ordinary people").

157. *See*, *e.g.*, WE THE PEOPLE, https://petitions.whitehouse.gov/petition/stop-all-animal-testing-cosmetics-and-household-products/TLdmJKBy (last visited Feb. 25, 2013); WE THE PEOPLE, https://petitions.whitehouse.gov/petition /investigate-abandoning-us-1-cent-coin-penny/fWczx9cm (last visited Feb. 25, 2013); WE THE PEOPLE, https://petitions.whitehouse.gov/petition/please-help-tonya-davis-meet-president-obama-her-last-wish-tonya-terminally-ill-and-needs-medical/jWGYBB1y (last visited Feb. 25, 2013); WE THE PEOPLE, https://petitions.whitehouse.gov/petition/bring-all-troops-home-afghanistan-december-31-2013/mnXBfssB (last visited Feb. 25, 2013).

158. *See, e.g.*, *No NHL Lockout*, IPETITIONS, http://www.ipetitions.com/petition/hockeyyinsiderr-no-nhl-lockout/ (last visited Feb. 25, 2013) (organizing a petition to end the NHL lockout).

159. Nicholas D. Kristof, Op-Ed., *After Recess: Change the World*, N.Y. TIMES, (Feb. 5, 2012), at 11.

160. *Id.*

161. *Id.*

162. *SOPA Petition Gets Millions of Signatures as Internet Piracy Legislation Protests Continue*, WASH.

how Google might use the personal information they entered (first and last name, email address, and zip code) learned through a pop-up prompt that Google would publish only signers' first names and last initials, and might use email addresses to send "updates" on Google's other policy initiatives.[163] Google thus assured signers that their political obscurity would remain intact through the public display only of first name and last initial. (Nonetheless, Google admitted that it would hold on to email addresses for future unspecified purposes.[164])

Attempting to harness online political energies, the White House has joined the online petitioning bandwagon too.[165] In September 2011, the White House launched a petitioning website called "We the People."[166] The site invites Americans to create and sign web petitions,[167] which are then submitted directly to the White House.[168] The White House pledges to respond to any petition that garners more than 25,000 signatures in a thirty-day window.[169] On some petitions, potential signers can see the names of others who have signed the petition, but the names are obscured to first name and last initial.[170]

POST (Jan. 20, 2011, 6:00 AM), http://www.washingtonpost.com/business/economy/sopa-petition-gets-millions-of-signatures-as-internet-piracy-legislation-protests-continue/2012/01/19/gIQAHaAyBQ_story.html.

163. *Take Action*, GOOGLE, https://www.google.com/takeaction (last visited Feb. 25, 2013). Clicking on the words "How we use your information" directly below the sign up box resulted in the following pop up: "The name that you give may be published publicly as part of this website and discussion. Your specified country and other location information may be used to display the vibrant conversation across the world. Your email address may be used to send you updates on Internet policy initiatives." *Id.*

164. *Id.*

165. *See We the People*, WHITE HOUSE, https://petitions.whitehouse.gov/ (last visited Feb. 25, 2013) (reading on its main page "[g]iving all Americans a way to engage their government on the issues that matter to them") *Id.*

166. *Id.*

167. Users must register and include their zip code, but the website does not require users to attest to their citizenship. *Create a WhiteHouse.gov Account*, WHITE HOUSE, https://petitions.whitehouse.gov/register (last visited Feb. 25, 2013).

168. *Step by Step Guide*, WHITE HOUSE, https://petitions.whitehouse.gov/how-why/step-step-guide (last visited Feb. 25, 2013).

169. *Id*. Petitions receiving responses from the White House range the full gamut of topics from re-establishing and maintaining a separation between commercial and investment banks to "[r]eleas[ing] all non-violent drug offenders" to "[a]ctually tak[ing] these petitions seriously instead of just using them as an excuse to pretend you are listening." Michael K, *Re-establish and Maintain the Separation Between Investment Banks and Commercial Banks*, WHITE HOUSE (Sept. 22, 2011), https://petitions.whitehouse.gov/petition/re-establish-and-maintain-separation-between-investment-banks-and-commercial-banks/ywCMKDfn; Adela F, *Release All Non-Violent Drug Offenders. Release All Inmates Who Are Incarcerated for Cannabis Related Crime*, WHITE HOUSE (Oct. 3, 2011), https://petitions.whitehouse.gov/petition/release-all-non-violent-drug-offenders-release-all-inmates-who-are-incarcerated-cannabis-related/tBvfwJC8; Scott S, *Actually Take These Petitions Seriously Instead of Just Using Them as an Excuse to Pretend You Are Listening*, WHITE HOUSE (Oct. 28, 2011), https://petitions.whitehouse.gov/petition/actually-take-these-petitions-seriously-instead-just-using-them-excuse-pretend-you-are-listening/grQ9mNkN. According to Macon Phillips, Director of the White House Office of Digital Strategy, the site is fast gaining traction. Macon Phillips, *We the People Update*, WHITE HOUSE (Sept. 4, 2012, 10:31 AM), http://www.whitehouse.gov/blog/2012/09/04/we-people-3-million-signatures-later.

170. *E.g.*, Michael K, *supra* note 169. The date of signing is also notated under the first name and last initial. The signer can indicate whether s/he would like to display city and state as well. *Id.*

Some criticize the White House platform as fluff, suggesting that it is no more than a public relations ploy.[171] A cynic might wonder whether the personal data that We the People collects was used to assist Obama's reelection (e.g., to gauge public opinion and identify potential supporters and critics).[172] But the relative success of the effort (according to the White House, the site averages 406 signatures per hour) underscores the ability of the Internet to harness political dynamism.[173] When compared to old-world petition signature gathering, there is no question that the Internet provides a previously unimaginable means to mobilize vast numbers of people quickly behind a cause.

Despite these strides, and amidst growing skepticism about the real impact of popular online petitioning as a political force,[174] the explosion of online popular petitioning does not necessarily indicate that individuals no longer value political obscurity. Several theories suggest that those who sign online popular petitions may not believe that signing threatens their political obscurity. First, many signers use fake identities when they sign online petitions. Because quality control and identity verification on online petitioning platforms are often weak, signers can sign online with created identities manufactured for the purpose. The signer may or may not be a citizen; the signer may or may not be of majority age.[175] These theories are supported by the structure of many online petitioning websites and the fact that they require minimal identifying information when signing.[176] For all we know Internet petitioners may be dogs.[177] Most online petitioning sites include only flimsy mechanisms to verify

171. *See* Joseph Marks, *White House Defends We the People Petition Responses*, NEXTGOV (Nov. 4, 2011), http://www.nextgov.com/nextgov/ng_20111104_3070.php (documenting generic White House responses to user allegations of indifference to the substance of petitions).

172. Others note that, by its terms, the site does not require real government action. Often the official response to "successful" petitions is nothing more than a letter stating the Administration's position. *Id*. According to the White House, as of September 4, 2012, 112 petitions crossed the threshold for response and twenty agencies/departments have authored responses. Phillips, *supra* note 169.

173. *See id.* (discussing how the site's popularity has "exceeded [White House] expectations").

174. Observers are starting to note downsides of online activism, suggesting that online petitions (and their cousins the mass-email campaign and campaigns that use social networking platforms like Facebook or Twitter) are "low-quality, redundant, and generally insubstantial commenting by the public." Stuart W. Shulman, *The Case Against Mass E-mails: Perverse Incentives and Low Quality Public Participation in U.S. Federal Rulemaking*, 1 POLICY & INTERNET 23, 26 (2009) (criticizing "the notion that online public participation is a harbinger of a more deliberative and democratic era."); *see also* Evgeny Morozov, *The Brave New World of Online Slacktivism*, FOREIGN POL'Y (May 19, 2009, 8:11 AM), http://neteffect.foreignpolicy.com/posts/2009/05/19/the_brave_new_world_of_slacktivism (describing slacktivism as the "feel-good online activism that has zero political or social impact"); Quentin Fottrell, *Petitions: From Constitutional Right to Online Joke*, WALL ST. J. MARKETWATCH (December 27, 2012), http://articles.marketwatch.com/2012-12-27/finance/36019500_1_online-petition-signatures-civic-act (describing online petitions that "more often veer off into frivolity or obscurity").

175. These theories are supported by the structure of many online petitioning websites and the fact that they require minimal identifying information when signing. See, for example, *supra* note 163 and accompanying text for a discussion of the information one provides when signing a petition on Google's Take Action website.

176. See *supra* note 163 and accompanying text for a discussion of the information one provides when signing a petition on Google's Take Action website.

177. *See* Peter Steiner, NEW YORKER, July 5, 1993, at 61 (New Yorker cartoon captioned: "On the Internet, nobody knows you're a dog").

identity—if true identity is verified at all.[178] The incentive to create a buzz with an Internet petition cuts heavily against any need to ensure that petition signers are who they say they are.[179] The ability to mask one's identity is one major difference between online popular petitioning and official petitioning, which places specific requirements on who is allowed to sign, contains mechanisms for signature verification, and imposes fines and/or criminal penalties for fraud.[180]

Second, for those who stand behind their identity on popular petitioning websites, it is unclear whether signers are aware that they are sacrificing political obscurity by signing. Online petition signers may not fully appreciate the uses of political preference data generated from such websites.[181] How many of the hundreds of thousands of people who have signed petitions at Change.org, for example, know that the company turns its profit by selling their names to groups that might be interested in marketing to people with the political preferences they indicate by signing? By clicking "Change.org for Organizations" at the bottom of the main page, and then clicking on "Change.org Premier Partner Program," the following plug to organizations interested in buying the names and contact information of Change.org petition signers appears:

> With Change.org's advertising platform, we enable agencies, consulting firms, and direct marketing companies to provide their clients with high quality supporters at an unprecedented scale. As a member of the Change.org Premier Partner Program, your company can better serve your clients by providing them the very best in supporter acquisition while expanding your reach in the nonprofit ecosystem.
>
> A few great reasons to become a Premier Partner
>
> - Receive the most cost effective pricing for supporter acquisition with preferred pricing
> - Maximize your client's ROI with the support of a dedicated

178. Many online petition sites require signers to register in order to add their name to the petition, relying on terms of service notifications that signers agree to provide accurate registration information. *See, e.g.*, *Terms of Service*, CHANGE.ORG, http://www.change.org/about/terms-of-service (last visited Feb. 25, 2013) ("By using the Service or the Site, you represent and warrant that you are 13 or older and that you agree to and to abide by all of the terms and conditions of this Agreement. . . . In consideration of your use of the Site, you agree to (a) provide accurate, current and complete information about you as may be prompted by any registration forms on the Site ('Registration Data') . . . .").

179. For example, in the SOPA petition, Internet activists encouraged non-U.S. citizens to create fake names and U.S. addresses to sign their petition. Gianluca Mezzofiore, *SOPA: Anonymous Extends OpBlackout Protest to non-US Citizens*, INT'L BUS. TIMES (Jan. 13, 2012, 10:29 AM), http://www.ibtimes.co.uk /articles/281259/20120113/sopa-anonymous-extends-opblackout-protest-non-citizens.htm.

180. *See, e.g.*, CAL. ELEC. CODE §§18600-14 (West 2012) (imposing a fine of not more than five thousand dollars and/or imprisonment for not more than three years); COLO. REV. STAT. ANN. §1-40-130(2) (West 2012) (imposing fine of not more than one thousand five hundred dollars and/or imprisonment for not more than one year); MD. CODE ANN., ELEC. LAW §16-401 (West 2012) (listing offenses related to petitions). Note that using a false identity could result in negative consequences for breaching petition sites' terms of service. *E.g.*, *Terms of Service*, *supra* note 178.

181. *See* Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCHOL. & PERSONALITY SCI. (forthcoming 2013) (manuscript at 2), *available at* http://www.futureofprivacy.org/wp-content/uploads/2010/07/Misplaced-Confidences-acquisti-FPF.pdf (hypothesizing that individuals are less concerned about others' eventual access to their personal information because the individuals control publication of that information).

Change.org client strategist

- Close more deals with the help of partner sales training, Change.org's sales and marketing toolkit, and access to our direct sales team
- Gain exposure to over 20,000 organizations using Change.org as their preferred action platform[182]

If online popular petition signers realized that petition sites are selling data about their political preferences, would they be dissuaded from indicating political preferences on online petitioning sites?

Third, other factors may explain why online petition signers—even those who use their real names and enter truthful personal information on online petitioning sites—feel that signing does not implicate their privacy interests. One may highly value political obscurity, but still subjectively believe that entering information on a petitioning website does not threaten it.[183] Unlike paper-based petitions, popular petition sites seldom allow users to view the full names and addresses of others who have signed the online petition nor will future potential signers see theirs. Again, an examination of Change.org may be instructive, as it gives signers the option to check a box that reads, "[d]isplay my signature publicly."[184] The assumption, if the box is not checked, is that the political preference signaled by signing the petition will remain private.[185]

In addition, unlike paper petitions most often circulated within a relatively circumscribed geographic area, online petitions are nationwide and in practice often exceed national boundaries.[186] The large geographic scale of online petitioning increases signers' sense of obscurity in a way paper petition signers do not experience when the circulator proceeds to the neighbor's house next.

Online petitioners also enjoy subjective privacy because no one else need *witness* their signature.[187] The individual who signs in his living room may feel his petitioning

182. *Change.org Premier Partner Program*, CHANGE.ORG, http://www.change.org/organizations/partners (Nov. 16, 2012).

183. For an interesting study of online website users' false sense of privacy, see Brandimarte et al., *supra* note 181.

184. *Privacy Policy*, CHANGE.ORG, http://www.change.org/about/privacy (last updated Oct. 25, 2012).

185. Change.org automatically creates a user profile when an individual signs a Change.org petition. *Terms of Service*, *supra* note 178. Users who click on a "Settings" tab are given the option to select "Privacy." *Privacy Policy*, CHANGE.ORG, http://www.change.org/about/privacy (last updated Oct. 25, 2012). The privacy settings do not allow users to restrict Change.org's use of user data. *Id.*

186. *See* Land, *supra* note 27, at 219 (describing Avaaz, an organization that uses technology and the internet to connect individuals across the world to influence global politics); *About*, *supra* note 156 (describing Change.org as the "world's largest petition platform" with over 20 million users in 196 countries). *See*, *e.g., Prosecute the Killer of Our Son, 17-year-old Trayvon Martin*, CHANGE.ORG, http://www.change.org/petitions/prosecute-the-killer-of-our-son-17-year-old-trayvon-martin (last visited Feb. 25, 2013) (showing 2,278,304 signatures from Canada, Thailand, and Hong Kong, among other places).

187. Online popular petition platforms have great flexibility in deciding when and whether signers' true identities are revealed. Some use this feature strategically. For example, on the UK website PledgeBank, users can pledge action only if others join. Users can pledge to start recycling if 100 people in their town do the same. *See* PLEDGEBANK, http://www.pledgebank.com/ (last visited Feb. 25, 2013) (using the tagline "I'll do it, but only if you'll help"). The question of whether or not signers' identifying information is revealed publicly,

activity is implicitly private—just as he might experience the requisite sense of privacy moments later when he enters his credit card data on Bed, Bath & Beyond's website to purchase new towels for his bathroom. Even if political data aggregators have a field day with online petition data—a remote threat to the average person—online petition signers can sign petitions when they are alone.

Subjective expectations of privacy are different when signing an online popular petition versus a real-world official petition; but this is starting to become less the case. As the next Part explores, new online forms of official petitioning may alter the privacy paradigm official petition signers' experience. In addition, like online popular petition signers, those who put their name to official petitions increasingly subject their political identities to a vast state cataloguing system that all but destroys political obscurity.

B. Modern Official Petitioning

Official petitioning, by its nature, is meant to be a clunky process. Official petitioning rests on the assumption that petitions should be relatively rare and used only for grave and important matters.[188] Official petitioning efforts must meet a certain threshold of toil to count; burdens on official petitioning function as a vetting mechanism.[189]

Burdens on official petitioning come in many forms. Aside from establishing minimum thresholds for how many signatures successful petitions must contain,[190] states impose many other forms of restrictions such as residency and other requirements on petition circulators,[191] and restrictions on petition content and form.[192]

however, is much different than the question of what petition sites do with signer data.

188. *See* Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182, 191–92 (1999) (discussing the import of the state interest in imposing restrictions on the petitioning process in order to improve its reliability); Louis J. Sirico, Jr., *The Constitutionality of the Initiative and Referendum*, 65 IOWA L. REV. 637, 659–66 (1980) (discussing official restraints on petition signature gathering imposed to ensure integrity and accurate representation of public support).

189. When Newt Gingrich and Rick Perry failed to get on the ballot in Virginia during the 2012 Republican primary, many saw it as indication that they lacked the will and organization to be presidential candidates. *See, e.g.*, Katharine Q. Seelye, *Gingrich Falls Short of Signatures Needed to Get on the Primary Ballot in Virginia*, N.Y. TIMES, Dec. 25, 2011, at A26.

190. Some states have even toyed with geographic restrictions on the topic of numerical targets. *See, e.g.*, Angle v. Miller, 673 F.3d 1122, 1127 (9th Cir. 2012) (upholding Equal Protection and First Amendment challenge to state ballot initiative geographic distribution requirement that proponents must obtain signatures from a number of registered voters equal to ten percent of the votes cast in the previous general election in each of the state's congressional districts).

191. *See, e.g.*, COLO. REV. STAT. ANN. § 1-40-112 (West 2012) (requiring petition circulators, *inter alia*, to be a resident of the state and at least eighteen years old); OHIO REV. CODE ANN. § 3503.06 (West 2012) (requiring circulators to be registered voters); 25 PA. CONS. STAT. ANN. § 2869 (West 2012) (providing that petitions must have an affidavit attached saying the circulator is a registered voter and other information).

192. *See, e.g.*, 10 ILL. COMP. STAT. ANN. 5/10-4 (West 2012) (detailing the form requirements of a petition); MICH. COMP. LAWS ANN. § 168.544c (West 2012) (providing the exact form a nominating petition must take); OR. REV. STAT. ANN. § 250.015 (West 2012) (requiring the secretary of state to design prospective petitions); 25 PA. CONS. STAT. ANN. § 2869 (West 2012) (prescribing specific formatting rules depending on type of candidate and whether multiple sheets are used). In one extraordinary recent example, the Michigan Supreme Court rejected a referendum petition because, though it contained enough valid signatures, the petition's heading was not fourteen-point font as required by Michigan statute. Stand Up for Democracy v.

Once circulators submit a petition to the state, the state scrutinizes petitions for signature validity and reserves the right to reject petitions if state-imposed burdens are not met.[193] Burdens on official petitioning are frequently challenged as overly onerous on First Amendment grounds: too many burdens on petition circulation violate the First Amendment much like overburdening citizens' ability to distribute handbills.[194]

In the past several decades, paid political consultants have taken a central role in official petition signature gathering. Many decry this development, worried that financial incentives have in many ways eclipsed "purer" political motivations.[195] Indeed signature gathering for official petitions has become a lucrative industry. Petition gatherers routinely earn one to four dollars per signature.[196] One or sometimes multiple political consultants operate in virtually every state to orchestrate petition drives.[197] Paying circulators for each signature they gather creates obvious incentive to forge names, "revive" deceased voters, or engage in other forms of fraud to get signatures.[198] Accusations of petition fraud are not new to the petitioning landscape, but

Sec'y of State, 822 N.W.2d 159, 181 (Mich. 2012).

193. *See, e.g.*, MICH. COMP. LAWS ANN. § 168.552 (West 2012) (providing extremely detailed rules for review, protests, and duties with regards to petitions); OHIO. REV. STAT. ANN. § 3513.263 (West 2012) (providing that "[w]ritten protests against such nominating petitions may be filed by any qualified elector eligible to vote for the candidate whose nominating petition the elector objects to, not later than the seventy-fourth day before the general election").

194. *See, e.g.*, Am. Party of Tex. v. White, 415 U.S. 767, 779–81, 788–91 (1974) (challenging time limit and residency requirements for petitions); Nader v. Brewer, 531 F.3d 1028, 1039–40 (9th Cir. 2009) (striking down residency requirement for petition gatherers); Lee v. Keith, 463 F.3d 763, 772 (7th Cir. 2006) (striking down as too burdensome an Illinois petition law requiring independent candidates to obtain ten percent of the total votes in the previous general election to obtain ballot access).

195. Joel Zuercher, *Democracy for Sale: The Signature Gathering Industry*, ACS BLOG (Aug. 20, 2004), http://www.acslaw.org/acsblog/democracy-for-sale-the-signature-gathering-industry; *see also* Daniel Hays Lowenstein & Robert M. Stern, *The First Amendment and Paid Initiative Petition Circulators: A Dissenting View and a Proposal*, 17 HASTINGS CONST. L.Q. 175, 176 (1989) (discussing the outrage following the invalidation of a state law banning circulators paid to qualify ballot initiatives). *But see* Drew Fitzgerald, *The Business of Signature Harvesting*, SUN CHRON., (June 14, 2010), http://www.thesunchronicle.com /articles/2010/06/14/news/7490389.txt (noting that "throwing money" at an unpopular initiative does not necessarily deliver results).

196. Fitzgerald, *supra* note 195.

197. When Americans Elect sought (unsuccessfully) to place a third party on the 2012 presidential ballot through an online primary, it reportedly paid a company called Arno Political Consultants $10.1 million to gather signatures throughout the country. *See* Center for Responsive Politics, *Americans Elect: Expenditures, 2010 Cycle*, OPENSECRETS.ORG, http://www.opensecrets.org/527s/527cmtedetail_expends.php?ein =272285014&cycle=2010 (last visited Feb. 25, 2013) (breaking down Americans Elect's expenditures during the 2010 election cycle); Scott Moore, *Americans Elect Part IV: Paying Big Money for Signatures*, OUR OREGON (Sept. 29, 2011), http://thesockeye.org/2011/09/29/sockeyeblogamericans-elect-part-iv-paying-big-money-signatures/ (providing a detailed report of Americans Elect's expenditures for signature gatherers). For a variety of reasons, the effort imploded. *See* Chris Cillizza & Aaron Blake, *Americans Elect and the Death of the Third Party Movement*, WASH. POST (May 18, 2012, 6:30 AM), http://www.washingtonpost.com/blogs/the -fix/post/americans-elect-and-the-death-of-the-third-party-movement/2012/05/17/gIQAIzNKXU_blog.html.

198. Jocelyn Friedrichs Benson, *Election Fraud and the Initiative Process: A Study of the 2006 Michigan Civil Rights Initiative*, 34 FORDHAM URB. L.J. 889, 896–97 (2007); Steve LeBlanc, *Marriage Backers, Foes, Point Fingers: Gay-Nuptials Ban Spawns Nastiness*, BOSTON GLOBE (Oct. 19, 2005), http://www.boston.com/news/local/massachusetts/articles/2005/10/19/marriage_backers_foes_point_fingers. Petition signature fraud has long been asserted and documented. In 1874, a Kansas court rejected a petition on

they are arguably exacerbated by these new petitioning realities.[199]

Responding to fears of fraud and to the problem of pay-to-play petition signature gathering, some states have begun to explore whether technology might be deployed as a possible fix.[200] If petitions can be signed online, cutting out the middleman, the paid petition circulator problem and many of the attendant fraud issues dissipate. While online petitioning is prohibited outright by statute in several states,[201] the increased use of technology to improve the process seems inevitable. We are unsurprisingly witnessing a growing movement to press states and municipalities to permit online official petitioning.

California was one of the first states to explore online official petitioning. In 2008, a proposal in California to allow online circulation for initiative petitions prompted the California-based Center for Governmental Studies (CGS) to evaluate the use of online official petitions.[202] CGS weighed the possibility of using "digital signatures" approved by the Secretary of State, plus a separate unique identifier sent to the voter by the Secretary of State, as a means of verifying online official petition signatures.[203] Although it cited security concerns, CGS found "no reason to believe that the problems of coercion or signature selling would be any greater for online signatures than for handwritten signatures on petitions circulated door-to-door or at shopping malls."[204] On the other hand, critics of the proposal worried online petition signing might make the initiative process *too* accessible by lowering the cost of participation so dramatically.[205] Ballot initiatives already overwhelm California voters; an easier process might make the number of initiatives not only unwieldy but contrary to the idea of representative government.[206]

By 2010, a California firm called Verafirma developed signature gathering

which over 600 names "were names of fictitious persons, minors, and non-residents, and names of resident electors signed thereto without their knowledge or consent." Butler v. McMillen, 13 Kan. 385, 386 (1874). In 1912, an Oregon court found sixty percent of signatures were forged or fraudulent on ballot initiatives. Todd Donovan & Daniel A. Smith, *Identifying and Preventing Signature Fraud on Ballot Measure Petitions*, *in* ELECTION FRAUD: DETECTING AND DETERRING ELECTORAL MANIPULATION 130, 143 n.6 (Michael R. Alvarez et al. eds., 2008). In Oklahoma in 1913, seven measures were removed from a ballot due to signature fraud. *Id.*

199. *See, e.g.*, Eric Shawn, *Indiana Lawmaker: Holder Absent on Petition Fraud Case*, FOX NEWS (Dec. 18, 2011), http://www.foxnews.com/politics/2011/12/18/indiana-lawmaker-holder-absent-on-primary-petition-fraud-case (reporting on a petition fraud in Indiana); *Dems Challenge 2008 McCain Petitions*, ONPOLITIX (Oct. 19, 2011), http://indiana.onpolitix.com/news/80737/democrats-challenge-2008-mccain-petitions (discussing 2008 presidential primary ballot challenges).

200. See *infra* notes 284–89 and accompanying text for a discussion of the recent petition verification efforts in Wisconsin for one such example.

201. *See, e.g.*, *Running for Office*, N.Y. STATE BD. OF ELECTIONS, http://www.elections.ny.gov/RunningOffice.html (last visited Feb. 25, 2013) (stating that the New York Board of Elections has expressly prohibited the use of e-signatures for official purposes).

202. WALTER S. BAER & ROY ULRICH, ONLINE SIGNATURE GATHERING FOR CALIFORNIA INITIATIVES 2–3 (2008).

203. *Id.* at 5–6.

204. *Id.* at 9–10.

205. *See id.* at 2 (noting that the ease of online petitioning could create a flood of ballot initiatives).

206. *Id.* at 14–15.

software to enable voters to sign petitions from a computer or smartphone.[207] The software allowed would-be petition signers to use a touchscreen device to trace their signature above their printed name and address after they viewed a copy of a petition on their screen.[208] The tracings would then appear on an electronic copy of the petition.[209] Hoping to prompt the State of California to accept e-signatures on petitions, Verafirma's founder, Michael Ni, brought a flash drive to the Board of Elections demanding the Board count the image of his signature contained on the drive in support of a ballot initiative legalizing marijuana.[210] When election officials refused, Ni sued for declaratory relief.[211] Ni's tactic did not pay off. The court held that e-signatures did not meet the statutory requirement that voters to "personally affix" their signatures on petitions.[212] For now, online official petitioning looks unlikely in the Golden State.

California is not the only state to ponder online petitioning. Nebraska considered a bill to allow voters to sign petitions online through a secure state election website,[213] but the legislature indefinitely postponed action on the bill in April 2012.[214] Utah has also toyed with electronic official petitioning. After a state court required state election officials to accept electronic signatures,[215] the legislature stopped the practice in its tracks, passing a law in 2011 that outlawed the use of electronic petition signatures.[216]

207. Mikeni8, *Verafirma – Sign Initiative Petitions with Your iPhone*, YOUTUBE (Dec. 8, 2009), http://www.youtube.com/watch?v=k1sdtiwCJ9s.

208. *Id.*

209. *Id.*

210. Kenneth Ofgang, *C.A. Rejects Bid to Count Online Signature on Initiative Petition*, METRO. NEWS-ENTERPRISE, (July 5, 2011), http://www.metnews.com/articles/2011/nixx070511.htm.

211. Ni v. Slocum, 127 Cal. Rptr. 3d 620, 622–23 (Cal. Ct. App. 2011).

212. *Id.* at 630.

213. Legis. B. 566, 102d Leg., 1st Sess. (Neb. 2011).

214. *See* NEBRASKA LEGISLATURE, LEGISLATIVE JOURNAL, 2d Sess., at 1562 (2012). Nebraska State Senator Paul Schumaker introduced the bill that would allow petition signers to go onto a website and input their name, county of residence, political party affiliation, date of birth, and a unique identifier that could be verified against other data. *Online Petition Signature Collection Proposed*, UNICAMERAL UPDATE (Mar. 3, 2011), http://update.legislature.ne.gov/?p=3659. The state would then send petition signers a postcard confirming his or her signature. *Id.* Additionally, the bill would provide criminal penalties for fraud. *Id.*

215. *See* Anderson v. Bell, 234 P.3d 1147, 1155–56 (Utah 2010) (holding that electronic signatures can be used to endorse candidate nominating because Utah statute did not require that the signature or other information be "personally affixed" to the petition). After the court handed down the decision mandating the acceptance of electronic signatures, the Lieutenant Governor Gregory Bell issued a rule requiring that petition circulators witness petition signatures. Joseph M. Dougherty, *E-Signature Rule May Face Challenge*, DESERET NEWS, July 11, 2010, at A1. Although Bell stated that organizers could use alternative methods, such as Skype, to witness online signers, the rule made it very difficult for organizers to use online signatures. *Id.* In any event, the issue was mooted by the legislature's action to ban online official petitioning. Robert Gehrke, *Legislature OKs Ban on E-signatures in Elections*, SALT LAKE TRIB. (Mar. 9, 2011), http://www.sltrib.com/sltrib /home/51395915-76/ballot-ban-bill-daw.html.csp.

216. Gehrke, *supra* note 215. In September, 2012, Utah activists promoted a referendum to overturn S.B. 165 to allow electronic petition signatures, hoping—ironically—to collect enough signatures to get on the ballot in November 2012. David Montero, *Cook Asks Supreme Court to Save Ballot Initiative*, SALT LAKE TRIB., Sept. 8, 2012, http://www.sltrib.com/sltrib/politics/54842717-90/ballot-case-cook-court.html.csp. Even more ironically, activists failed to collect enough signatures to place the measure on the ballot in 2012. *See* David Montero, *Judge Rules Against Foes of Utah's Initiative Law*, SALT LAKE TRIB., Sept. 2, 2012, http://www.sltrib.com/sltrib/news/54806753-78/ballot-cook-law-court.html.csp. (noting that activists were so

Montana has also addressed the e-signature question and seems amenable to the idea.[217]

But the most interesting action in online petitioning is taking place in Maryland. In 2011, organizers of a Maryland petition undertook a referendum opposing the state's DREAM Act.[218] To collect those signatures, Republican State Delegate Neil Parrott created a website called MDPetitions.com.[219] To use the site, which Parrott promoted on talk radio and other news outlets,[220] voters enter basic information, including first and last name, email address, phone number, date of birth, and zip code.[221] The site then displays the name of the user entering the information, plus the names of all the members of his or her household.[222] The site directs the user to check a box next to the names of all members of the household willing to sign the petition.[223] The site then directs the user to download the petition, at which point MDPetitions software generates a petition form, populated with names and required information of all individuals in the household, and space for each to sign.[224] Voters then print the petition form, sign it (and have other household members sign).[225] The printed form also includes a separate section on which the signer signs and dates the form as the circulator (i.e., the signer acts as his or her own witness/circulator).[226] Signers then must send their completed petition forms via mail to MDPetitions in Funkstown, MD.[227] The organization then amasses the printouts and delivers them to the State Board of Elections for certification.[228]

During the DREAM Act petition effort, the Maryland ACLU and other groups challenged the validity of online signatures, voicing concern that the system contained insufficient checks to detect fraud.[229] The State Board of Elections, however, opted to

many signatures short, they would not be able to gather enough signatures before the deadline to place it on the ballot).

217. In the wake of the Utah electronic petition signature controversy, the Montana Attorney General's office issued an advisory letter noting that because of the structure of Montana's adoption of the Uniform Electronic Transactions Act (different from the version adopted in Utah), the state's Board of Election maintains discretion to count e-signatures. Letter of Advice from J. Stuart Segrest, Montana Assistant Attorney General, to Linda McCulloch, Montana Secretary of State (July 25, 2011).

218. S. 167, 2011 Leg. Reg. Sess. (Md. 2011). The Development, Relief and Education for Alien Minors (DREAM) Act would have provided conditional permanent residency to certain illegal aliens, most recently approved by the governor in May 2011. David Hill, *Petitioners Boasting 100,000 Signatures; Dream Act Foes Put Law on Hold*, WASH. TIMES, July 1, 2011, at A16. Opponents submitted enough signatures to delay the enactment of the bill. *Id.*

219. Camille Eslick, *Petitioning Goes Online: Initiative and Referendum Consultants See Potential in the Drive for Verified Signatures Online*, CAMPAIGNS & ELECTIONS, July/Aug. 2011, at 48–49.

220. *Id.* at 49.

221. Complaint for Declaratory and Injunctive Relief at 9, Whitley v. Md. State Bd. of Elections, No. 02-C-12-171365 (Md. Cir. Ct. for Anne Arundel Cnty. Aug. 10, 2012).

222. *Id.*

223. *Id.*

224. *Id.* at 9–10.

225. *Id.*

226. *Id.*

227. *Id.* at 9.

228. For the successful DREAM Act petition, Parrott ultimately collected about one-third of his petition signatures online. Eslick, *supra* note 219, at 48–49.

229. David Hill, *State ACLU Challenges E-Signature Petitions: Says Dream Act Vote Website Violates*

certify the electronic signatures and has blessed the collection of petition signatures in this fashion.[230] Since that time, the MDPetitions website has expanded to include a variety of petitioning efforts.[231]

In July 2012, the Maryland State Democratic Committee, responding to MDPetitions's effort to put a redistricting map on the general election ballot in November 2012,[232] challenged the collection of online signatures in the Circuit Court for Anne Arundel County.[233] The complaint alleged that the online petition process encourages fraud because signers witness their own signature.[234] In addition, the complaint argued that signatures collected online should be invalidated because MDPetitions pre-fills the petition forms in violation of a Maryland statute that plaintiffs claimed required each signer to complete him or herself.[235] Ultimately, the court upheld the online petitioning process, ruling the practice meets Maryland statutory requirements.[236]

Maryland's online petition system has huge advantages for political organizers seeking to gather signatures.[237] Rather than standing on street corners trying randomly to identify those who may or may not be sympathetic to their political position, organizers only have to direct known supporters to a website. Political organizers can purchase targeted lists from companies described above to increase their chances of targeting sympathetic eyeballs and can construct pinpointed email and social media campaigns to proposition likely signers.[238]

By cutting out the middleman, Maryland's new method alters the privacy paradigm. In Maryland, one can now sign an official petition from the privacy of one's own home without a grocery store sidewalk interaction or other public interface.

the Law, WASH. TIMES, July 30, 2011, at A15. Opponents of ACLU's position noted that the MD ACLU's arguments were undercut by the Utah ACLU's support of online petitioning. *Id.*

230. The immigrant advocacy group Casa de Maryland later dropped its challenge to the validity of the signatures. David Hill, *Immigrant Group Drops Petition Challenge*, WASH. TIMES, Dec. 9, 2011, at A16. The challenge was in some ways a losing battle since the Maryland election board determined the group had collected nearly 109,000 valid voter signatures, roughly double the 55,736 signatures needed. *See* David Hill, *Immigrant Group Sues to Uphold Dream Act*, WASH. TIMES, Aug. 2, 2011, at A14 (reporting on invalidated petition signatures, leaving petitioners 4,000 signatures short of the threshold).

231. *See* MDPETITIONS.COM, http://www.mdpetitions.com (last visited Feb. 25, 2013) (adding redistricting and same-sex marriage to the list of successful petitions).

232. Pursuant to Maryland Constitution, voters can refer an act passed by the General Assembly to referendum by voters if they collect a petition signed by a number of qualified voters equal to three percent of the whole number of votes cast for Governor at the last preceding gubernatorial election. MD. CONST. art. XVI, § 3.

233. Complaint for Declaratory and Injunctive Relief, *supra* note 221, at 2.

234. *Id.* at 12–13.

235. *See* MD. CODE REGS. 33.06.03.06(B) (2012) (stating that "each signer shall . . . (2) Provide the following information, to be printed or typed in the appropriate spaces: (a) Date of signing, (b) Signer's name as it was signed, and (c) Current residence address, including house number, street name, apartment number (if applicable), town, and ZIP code").

236. Whitley v. Maryland State Bd. of Elections, No. 02-C-12-171365 (Md. Cir. Ct. for Anne Arundel Cnty. Aug. 10, 2012), *aff'd* 50 A.3d 9 (Md. 2012).

237. BAER & ULRICH, *supra* note 202, at 2.

238. *See* Duhigg, *supra* note 115 (explaining how companies use personal information they acquire to target potential customers).

Though the signature must still be sent to the group organizing the petition drive, Americans are used to sending confidential documents through the mail—it *feels* more private than a face-to-face interaction. This development, if it is mimicked in other states, could radically alter our subjective experience of political privacy in official petitioning that mirrors subjective privacy expectations in the popular petitioning realm.

While MDPetitions may enhance signers' subjective sense of privacy, that security is misplaced. Data about the activities of Maryland's petitioning public has never been more carefully catalogued or more freely available.[239] Once an organization has collected signatures (online or on paper), those signatures are delivered to the Maryland State Board of Elections for verification.[240] In many states—particularly larger ones—the petition signature verification process consists of random spot checks, leaving the onus on those opposed to a petition to prove the documents contained invalid signatures.[241] In Maryland, however, not only is every signature verified,[242] but the fact of one's signing a petition becomes a permanent record on the state's voter registry.[243] As required under the Help America Vote Act, Maryland created a centralized voter registry called the Statewide Voter Registration System (MDVOTERS).[244] MDVOTERS, in addition to creating a central voter registry, also includes features for coding individual names with information about petitioning activity.[245] Election officials now verify petition signatures on MDVOTERS by adding a code beside each signer's name indicating which petitions that voter signed, whether or not officials deemed the signature valid, and if invalid, the reason the signature failed to pass muster.[246]

239. But see *infra* note 251 and accompanying text for a description of the 2013 legislative efforts to curb access to petition data in Maryland.

240. Historically, petition organizers submitted petitions grouped by county so that the Maryland State Board could then farm signature sheets out to individual counties for verification. Telephone Interview with Jared DeMarinis, Director, Division of Candidacy and Campaign Finance, Maryland State Board of Elections (Aug. 3, 2012). The State Board still maintains the practice of sending forms to counties to verify, but this practice is no longer necessary from a practical standpoint because Maryland's voter registry is now centralized. *Id.*

241. For example, in the State of Washington, the secretary of state has the burden. *See* WASH. REV. CODE ANN. § 29A.72.230 (West 2012) ("The secretary of state may use any statistical sampling techniques for this verification and canvass which have been adopted by rule as provided by chapter 34.05 RCW.").

242. At least until the required threshold is reached.

243. If the signature verification process determines that the required number of valid signatures have been collected, the remaining signatures may go unverified and uncoded. Telephone Interview with Jared DeMarinis, *supra* note 240.

244. 42 U.S.C. § 15483(a)(1)(A) (2006) ("[E]ach State, acting through the chief State election official, shall implement, in a uniform and nondiscriminatory manner, a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State . . . ."). Previously, individual Maryland counties had been responsible for maintaining their own voter lists. Janet Stidman Eveleth, *Managing Maryland Elections*, MD. B. J., Sept.–Oct. 2000, at 2, 7.

245. MD. ST. BOARD OF ELECTIONS, PETITION ACCEPTANCE AND VERIFICATION PROCEDURES 2–6 (2012).

246. For example, "NS" if the name is not written in standard form; "DUP" if the name is duplicated on

As a result of its digitized system, the state board can generate lists of individuals who have signed specific petitions, lists of individuals whose names have been validated or invalidated for signing specific petitions, and the reasons for disqualification. Should a member of the public request, the board can generate a list of all the petitions a specific voter or group of voters has signed. The result is a substantial loss of political obscurity in Maryland. In the past, it would have been very difficult to ferret out the names of petition signers, and even harder (if not impossible) to determine what petitions a particular individual had signed. Now the process may unfold with a few strikes on a keyboard.

Political organizers will enjoy benefits from decreased political obscurity. Although MDPetitions could dramatically impact the signature-gathering industry's bottom line, some in the industry praise the idea because the process promises better political data. Observed one petition signature gathering consultant of Maryland's online petitioning, "[i]f voters go out of their way to fill out, print and then mail their petition signature, the quality of the signers is better, meaning a richer database to call upon down the road."[247]

Unsurprisingly, following KnowThyNeighbor.org's lead, a prominent LGBT newspaper in Washington, D.C., *The Washington Blade*, uploaded a searchable list of the names and addresses of those who signed the Maryland anti–gay marriage petition, again cross-referencing Google Maps to allow individuals the ability to figure out who had signed in their locality.[248] Some hailed the move as a means of assuring political accountability in Maryland; others were less sure.[249]

another signature page; "CG" if the signer signed via computer generated petition; and "SI" for failure to provide signature or address. *Id.* at 8. Note that Maryland's digitizing of petition signatures resulted in confusion on Election Day in 2012. When Marylanders signed petitions using a different address than what appears on their voter registration, the discrepancy prevented voters from casting a regular ballot. *See* Erin Cox, *Officials Investigate Long Lines at Polls: Area Voters Dissatisfied by Extended Waits, Names Missing from Rolls*, BALTIMORE SUN, Nov. 8, 2012, at 2A (describing Maryland resident Christopher Lochner who, having signed a petition using a different address than his voter registration address, was forced to vote provisionally). Maryland legislators responded by introducing a bill in January 2013 that would require signers to use the same address as on their voter registration, and would prevent the state board from using petition addresses to update voter registration records. *See* H.D. 493, 2013 Leg., 430th Sess. (Md. 2013).

247. Eslick, *supra* note 219, at 49.

248. WBadmin, *Who Signed the Md. Anti-Gay Marriage Petition?*, WASH. BLADE (July 25, 2012), http://www.washingtonblade.com/2012/07/25/who-signed-the-md-anti-gay-marriage-petition/.

249. Tom Lang, Director of KnowThyNeighbor.org, commented on the *Washington Blade* piece:

> To LGBT and allies, look to signers in Maryland and you will find friends and family members, people you employ and owners of establishments you patronize. Now and in the years to come, you will find also, politicians running for office who may or may not have a good enough answer as to why he or she signed this initiative to take away rights. And know . . . once you see names your [sic] recognize . . . your true work begins.

Tom Lang, Comment to *Who Signed the Md. Anti-Gay Marriage Petition?*, WASH. BLADE (July 25, 2012, 3:19 PM), http://www.washingtonblade.com/2012/07/25/who-signed-the-md-anti-gay-marriage-petition/#comment-59345. Another commenter was less sure:

> [P]ublishing people who signed it does bother me. I think we need to encourage people to be part of the democratic process and posting their information sets them up for their rights to be violated, and let's be honest we are all suppose [sic] to be supporting equal rights for all and not targeting individuals who disagree with us or we are NO better.

The loss of political obscurity for Maryland petition signers had real consequences in 2012. In one prominent example, a Maryland university placed its chief diversity officer on administrative leave after learning online that she had signed the anti–gay marriage petition.[250] But aside from this high-profile example, the real question is whether Maryland petition signers will now think twice before adding their name to petitioning efforts in a climate in which political obscurity in petition signing is effectively gone. It seems the Maryland legislature is concerned. In its 2013 session, members are considering a slew of bills that would curb both online petitioning and disclosure of petition signatures.[251]

In both the popular and official realm, signing a petition today potentially exposes individuals to a form of state political cataloguing on a scale, in formats, and for purposes never contemplated by the authors of our democracy. The Internet has shaken the traditional balance between protecting political obscurity and requiring public accountability. Unless courts, legislatures, and administrators recognize the state's role in shaping this reality and take steps to recalibrate the balance, participation in official petitioning is threatened. The next Section explores what might be done.

V. PROTECTING POLITICAL OBSCURITY IN MODERN OFFICIAL PETITIONING

The nominally public nature of official petition signing should not negate an individual's interest in maintaining political obscurity in a modern age when information is fluid, amplified, and permanent. After its foray into more technologically creative petitioning practices, Maryland may choose to move in the direction of a state known for protecting the privacy of its citizens: California.[252] California takes a particularly protective view of official petition signer privacy. In California, only named proponents of official petitions are entitled to examine signatures to ascertain which the Secretary of State disqualified and the reason(s) for disqualification.[253] The right of examination exists only for a twenty-one-day period after certification of insufficiency of signatures.[254] Review of petition signatures is not

James, Comment to *Who Signed the Md. Anti-Gay Marriage Petition?*, WASH. BLADE (July 31, 2012, 5:13 PM), http://www.washingtonblade.com/2012/07/25/who-signed-the-md-anti-gay-marriage-petition/#comment-60400.

250. Joan Frawley Desmond, *Targeted Public Disclosure Laws? Opponents of Same Sex Marriage Feel the Heat*, NAT'L CATHOLIC REG. (Oct. 31, 2012 2:11 PM), http://www.ncregister.com/site/article/targeted-by-public-disclosure-laws. The university reinstated the diversity officer three months later in January 2013. *Angela McCaskill Reinstated: Gallaudet University Diversity Officer Returns Three Months After Signing Anti-Gay Marriage Petition*, HUFFINGTON POST (Jan. 8, 2013, 2:01 PM), http://www.huffingtonpost.com/2013/01/08/angela-mccaskill-reinstated-gallaudet_n_2432838.html.

251. *See, e.g.*, Referendum Integrity Act, H.B 493, 2013 Leg., 430th Sess. (Md. 2013) (making online petition signature gathering more difficult by placing restrictions on who can circulate an online petition and what that petition must contain); H.B. 49, 2013 Leg., 430th Sess. (Md. 2013) (allowing public inspection of signatures "to facilitate judicial review of a determination concerning the sufficiency of the petition [signatures]," but forbidding the state otherwise from releasing personal information contained in a petition to the general public).

252. Margaret Betzel, Comment, *Privacy Law Developments in California*, 2 ISJLP 831, 831 (2006) (noting that "California has led the nation in the development of privacy laws").

253. CAL. GOV'T CODE § 6253.5 (West 2012); CAL. ELEC. CODE § 11301.

254. CAL. GOV'T CODE § 6253.5.

available to the public generally, including those who signed the petition.[255] California statute further renders accessing petition signatures for use other than the original purpose, a misdemeanor.[256] Most states are far less protective of petition signer privacy. Wisconsin, at the other end of the spectrum, has, in the case of the high-profile Scott Walker recall, affirmatively posted petition signature pages on a government website.[257] Most states, however, fall in between these two extremes, allowing public access to petition signatures through public records requests. The extent to which states should re-examine these rules to take into account the changed information technology landscape is the question to which this Section now turns.

Official petitioning custodianship is difficult. But official petitions are not the first type of public document to face the challenge of digital dissemination of information. Court records provide an example of a public document system that has undergone great transformation in the last decade.[258] Just like official petitions, court records are also presumed to be public.[259] But the right of public access to court records has historically been greatly limited by practical realities. Before the Internet, "members of the public had no choice but to trudge to the courthouse to obtain access to records from the clerk."[260] Beginning in the early 1990s, judges and court administrators confronted the reality that public court records could be made easily available to the public on the Internet.[261] Since then, policymakers have debated whether court access policies should be altered in light of new and changing technological realities.[262] Many have argued that "'public is public'—i.e., if a document is public, it should be made available online as well."[263] The "public is public" camp believes that giving the public

255. *Id.*

256. CAL. ELEC. CODE § 18650.

257. *See, e.g.*, *Home: Recall Petitions*, WISC. GOV'T ACCOUNTABILITY BD., https://webapps.wi.gov/sites/recall/default.aspx (last visited Feb. 25, 2013) (providing signature pages for Wisconsin recall petitions).

258. Alan Carlson, *Public Access to Court Records: Reducing the Risk of Disclosure of Personally Identifiable Information*, *in* FUTURE TRENDS IN STATE COURTS 2007 19, 19 (Carol R. Flango et al. eds., 2007).

259. Despite an absence of explicit language in the Constitution guaranteeing public access to records, the right of access stems from the historical evolution of the justice system. Since the time of the Norman Conquest, open access to trials served a fundamental set of purposes, such as discouraging perjury and misconduct and ensuring against biased decision making. Robert Hardaway & Douglas B. Tumminello, *Pretrial Publicity in Criminal Cases of National Notoriety: Constructing a Remedy for the Remediless Wrong*, 46 AM. U. L. REV. 39, 40 (1996). The presumption of openness is not limited to the criminal context. While no constitutional proclamation safeguards the access to civil proceedings, the Supreme Court has recognized a common law right of access to civil proceedings as well. *See* Publicker Indus., Inc. v. Cohen, 733 F.2d 1059, 1070 (3d Cir. 1984) (finding a right of public access to civil trials). Building on this history of openness is the public's right to "inspect and copy public records and documents, including judicial records and documents." Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978) (footnote omitted).

260. Rebecca Hulse, *Privacy and Domestic Violence in Court*, 16 WM. & MARY J. WOMEN & L. 237, 258–59 (2010).

261. *Id.*

262. From January 2001 to July 2002, an advisory panel created by the National Center for State Courts met to study access to electronic court records and develop model guidelines to be applied to state court systems. Martha Wade Steketee & Alan Carlson, *Privacy and Public Access to Court Records: Public and Private Dimensions Create a Diverse Group of Collaborators*, *in* 2002 REPORT ON TRENDS IN THE STATE COURTS 23, 23 (2002).

263. Hulse, *supra* note 260, at 259.

more meaningful and convenient access through the Internet upholds and forwards the values that underlie transparency and the presumption of openness.[264]

Others believe that amplified online access to court records demands a major shift in policy and practice. Privacy interests of litigants (and nonlitigants, such as witnesses) once protected by dusty and hard-to-access court files would be thrust out there for all to see if posted online, requiring new policies to protect litigants' privacy interests in this new information landscape.[265]

Following the conversion from paper to electronic records in the 1990s, some jurisdictions put digitized court records online in wholesale fashion. Since the underlying documents are public, like the signatures in *Doe v. Reed*, the move seemed like a no-brainer.[266] In some cases, however, wholesale online publication of public court records proved disastrous.[267] An example from Oklahoma is illustrative. In early March 2008, following "public is public" reasoning, Oklahoma court administrators elected to place nearly nine million unredacted public court records online.[268] Unsurprisingly, administrators quickly faced harsh criticism when members of the media discovered Social Security numbers and other personally identifiable information of various Oklahoma public figures on the court's website.[269] A few weeks later, the Oklahoma Supreme Court reacted, adopting rules that flatly prohibited online

264. *Id.* This is largely the approach taken by the federal judiciary. *See* PUBLIC ACCESS TO COURT ELECTRONIC RECORDS, http://www.pacer.gov (last visited Feb. 25, 2013) (providing electronic public access service to case and docket information from federal appellate, district, and bankruptcy courts). One reason that the federal judiciary had less to fear from putting records directly online may be that the most sensitive personal data found in court records systems—family and juvenile cases, for example—are heard predominantly at the state level. *See* Hulse, *supra* note 260, at 267–68 (explaining that most state court records are not usually available online, with only basic docket information such as the names of the parties available electronically); Winn, *supra* note 29, at 148–49 (explaining the state court system's preference for solving the disputes and helping the parties rather than serving an abstract public interest). The Reporters Committee for Freedom of the Press usefully compiles a list of electronically accessible records for each state. *State-by-State Guide*, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, http://www.rcfp.org/access-electronic-communications/state-state-guide (last visited Feb. 25, 2013).

265. *See* Winn, *supra* note 29, at 138 (stating that judges at times have access to highly confidential information that should not be made public).

266. PACER's pay wall restores some measure of practical obscurity. See *infra* note 278 and accompanying text for a discussion of Pacer and the digitization court records.

267. *See* Winn, *supra* note 29, at 151 (discussing audit of PACER documents revealed unredacted social security numbers on hundreds of in-court pleadings).

268. Mike McCarville, MCCARVILLE REPORT ONLINE (Mar. 11, 2008, 3:52 PM), http://wwwtmrcom.blogspot.com/2008/03/oklahoma-county-clerks-records-reveal.html.

269. *See id.* (quoting an article from *The Oklahoman* that discussed Oklahoma County Clerk Carolynn Caudill's efforts to make all county records available online).

> Almost all of some 8.7 million documents—17 million pages—are online, from mortgage documents, mineral deeds, liens and other legal 'papers,' from original land patents granted after the Land Run of 1889 to last week's property deals, said Mark Mishoe, chief deputy for County Clerk Carolynn Caudill . . . . The conversion cost about $2.5 million—from a $5 fee assessed since 2000 on most documents filed.

Id. See also John Greiner, *High Court Backs Off Secrecy Rules*, OKLAHOMAN, Mar. 26, 2008, at A1 (discussing the Oklahoma Supreme Court as stating their holding as an attempt to balance the privacy rights of individuals and public access to court documents).

access to court records.[270] Many other states have struggled with this issue, thinking twice about making records too available online.[271]

Most courts, however, have refrained putting records online wholesale, in an attempt to retain some measure of practical obscurity in court records. Over the course of the past decade, courts and judicial administrators have developed inventive strategies that move away from an open/closed, public/private dichotomy. Many have explored the difficult question of redaction.[272] Others have looked at making only some portions of the court file available online.[273]

One of the more interesting approaches is the formation of an entirely new category of access termed "courthouse-only."[274] Some courts have determined that certain court records (or information contained within those documents) are, either by courthouse rule, state statute, or in rare instances by federal statute,[275] inappropriate for release on the Internet, even though that same document or the information within it is publicly available at the courthouse.[276] Courts maintaining a "courthouse-only"

270. Greiner, *supra* note 269. A few weeks later, on March 25, 2008, under fire from access advocates, the Oklahoma Supreme Court withdrew the order to "give the issue further study and consideration." *Id*. Since 2008, Oklahoma has moved to revise its policy. *See* Omer Gillham, *Tulsa County Begins Posting Court Documents Online*, TULSA WORLD, Dec. 27, 2011, at A11 (discussing the Oklahoma Supreme Court approval of rules clarifying when identifiers such as birth dates, home addresses, and Social Security numbers will be redacted).

271. For example, in 2010, fearing that too much sensitive private information from court records was finding its way online, a Montana state law librarian filed a petition with the state supreme court asking that the presumption of openness be overturned. The Montana Supreme Court agreed and suspended the presumption of openness. *In re* Temporarily Suspending the Rules for Privacy and Public Access to Court Records in Montana, No. AF 06-0377 (Mont. Sept. 14, 2011).

272. Court redaction software has become a cottage industry as private companies seek to provide a technological fix to the problem of retroactively redacting public court records. Laura Gater, *Intelligent Redaction Technology*, COMPUTING SYS. INNOVATIONS, May/June 2005, http://www.csisoft.com /applications/courts_today_article.pdf. It has in many ways been an uphill battle. A 2008 audit of the federal judiciary's PACER system revealed more than 1600 cases with redaction failures. Timothy B. Lee, *Studying the Frequency of Redaction Failures in PACER*, FREEDOM TO TINKER (May 25, 2011), https://freedom-to-tinker.com/blog/tblee/studying-frequency-redaction-failures-pacer.

273. For example, states like Washington have experimented with the "confidential coversheet" approach. In family law and guardianship cases, all sensitive personal information is placed on a confidential coversheet that is not released to the public, online or otherwise, even if the rest of the file is publicly accessible. *See* WASH. GEN. APPLICATION CT. R. 22(e) (explaining that the confidential cover sheet will be under the seal of the court). Some are pursuing sophisticated technological approaches that would place information within court records in separate fields that could be coded with catered privacy protections. *See* Diana Graski & Thomas M. Clarke, *Automating the Enforcement of Privacy Policies*, *in* FUTURE TRENDS IN STATE COURTS 2012 155, 157 (Carol Flango et al. eds., 2012) (stating there are multiple benefits to acquiring sophisticated technology to code documents).

274. Carlson, *supra* note 258, at 20.

275. For example, the Violence Against Women Act prohibits the publication on the Internet of identifying information in protective orders and restraining orders. 18 U.S.C. § 2265(d)(3) (2006) ("A State, Indian tribe, or territory shall not make available publicly on the Internet any information regarding the registration, filing of a petition for, or issuance of a protection order, restraining order or injunction . . . in either the issuing or enforcing State, tribal or territorial jurisdiction, if such publication would be likely to publicly reveal the identity or location of the party protected under such order.").

276. The Conference of Chief Justices/Conference of State Courts Administrators Guidelines suggest such an approach in section 4.50. Carlson, *supra* note 258, at 20. A 2007 survey indicated that twelve out of

approach will often provide a computer kiosk (or several) in the clerk's office at which the public can search for the record sought.[277] Members of the public still enjoy the efficiencies of digital records, but must expend effort to access those records by making the trip to the courthouse.[278] The strategy is similar to a municipality installing a speed bump. Here, rather than slowing cars down, the attempt is to restore some measure of practical obscurity.[279] Doing so has been critically important in the court records context. The fear, voiced by many in the judiciary and made real by the dramatic rise in the use of "private justice" mechanisms to escape public glare, is that the public will shy away from using courts to resolve disputes.[280] In the case of court records, the arrival of the Internet has forced judges and court administrators to rethink old black-and-white policies, and in some instances, install speed bumps to restore practical obscurity.

Speed bumps are needed to ensure political obscurity in the petitioning context as well. Rather than adopting a "public is public" approach, releasing petition signatures and identifying information in full, legislatures and state administrative agencies responsible for managing the official petitioning process should explore policies that reflect changing data-privacy realities. If transparency and integrity of the petitioning

twenty-two courts reviewed employed the courthouse-only strategy. *Id.*

277. *See, e.g.*, ADMIN. OFFICE OF THE ILLINOIS COURTS, ELECTRONIC ACCESS POLICY FOR CIRCUIT COURT RECORDS OF THE ILLINOIS COURTS § 4.30 (2004) (listing items that, while public, are not made available in electronic form but may be accessed at the office of the clerk of court). Note that the "courthouse-only" option is enshrined in the CCJ/COSCA Model Policy for access to electronic court records. Carlson, *supra* note 258, at 20.

278. The fluidity of data today, however, complicates easy fixes. For example, the federal digital court records site PACER put court records behind a pay wall. Registering its opposition to the PACER charges for access to public court records, an organization called RECAP enabled PACER users to download accessed documents to a site where those public documents were available for free. *About*, RECAP, https://www.recapthelaw.org/about/ (last visited Feb. 25, 2013). It would be similarly possible to circumvent "courthouse only" policies by simply sending someone to the courthouse to download records and then post those records online. For example, the Environmental Protection Agency tried to get around this problem by creating "reading rooms." Letter from John B. Stephenson, Director, GAO Natural Resources & Environment, to W.J. "Billy" Tauzin, House of Representatives & John Shimkus, House of Representatives 3 (March 14, 2003). The chemical manufacturing industry is required to report information to the federal government. *Id.* After 9/11, many worried that making such documents available to the public posed national security risks. *Id.* Others maintained that access to this information was crucial to providing public oversight of the industry. As a compromise, the EPA created special reading rooms, in which individuals "may read facility . . . information, but may not mechanically reproduce or remove this information from the reading room." *Id.*

279. Many people still fly over speed bumps, undaunted. The same is true of course in the case of court records. Once information is made public, it is often very difficult to stop it from spilling out onto the Internet. *See, e.g.*, *About*, *supra* note 278 (serving as an example of court records being posted on the Internet once they are made public).

280. *See, e.g.*, Laurie Kratky Doré, *Public Courts Versus Private Justice: It's Time to Let Some Sun Shine in on Alternative Dispute Resolution*, 81 CHI.-KENT L. REV. 463, 465 (2006) (finding "increased transparency in civil litigation may have wrought an unintended and unwelcome consequence—the diversion of more civil disputes into alternative dispute resolution proceedings like arbitration, where the public is 'shut out of information almost completely'" (quoting Jack B. Weinstein & Catherine Wimberly, *Secrecy in Law and Science*, 23 CARDOZO L. REV. 1, 20 (2001))); Stephanie Brenowitz, Note, *Deadly Secrecy: The Erosion of Public Information Under Private Justice*, 19 OHIO ST. J. ON DISP. RESOL. 679 (2004) (demonstrating how public access to important information under traditional litigation is being eroded by private judicial mechanisms).

process is the goal, wholesale posting of petitions online may not be the best means of promoting it.[281] Why not permit the public to inspect copies of petition signatures at computer kiosks maintained at the state agency responsible for administering the petitioning process? For a relatively low cost, states could provide concerned citizens with a mechanism to review not just the names of petition signers, but also images of the signatures themselves. The state could provide automated tools by which citizens could cross-reference signatures with the state's voter registration database in addition to any number of other applications that might assist members of the public in verifying the validity of petition signatures far short of the crude mechanism of posting wholesale online.[282] The government can and should do better, using modern tools at its disposal, to give the public an efficient means to oversee the petitioning process.[283]

In addition to these speed bumps, states could take a cue from online popular petitioning sites to protect signer obscurity. For example, signers of petitions could

281. Any move to restrict access outright to petition signatures is undesirable as a policy matter, given the need for transparency and oversight in petitioning, and because doing so violates the First Amendment. *See, e.g.*, Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058, 1088 (9th Cir. 2002) (holding that portion of site listing the names and addresses of doctors who perform abortions enjoys First Amendment protection); Brayshaw v. City of Tallahassee 709 F. Supp. 2d 1244, 1250 (N.D. Fla. 2010) (finding Florida statute proscribing publication of police officer's home address or telephone number violated First Amendment); United States v. Carmichael, 326 F. Supp. 2d 1267, 1270 (M.D. Ala. 2004) (finding that blocking a website containing publicly accessed information about government informants would violate First Amendment). However, just because information is public does not mean that the most convenient method of access is required. *See* U.S. Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 779–80 (1989) (holding disclosure of an FBI rap sheet to a third party "could reasonably be expected to constitute an unwarranted invasion of personal privacy"); Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 609–11 (1978) (holding that press is not entitled to tapes containing incriminating recordings of Nixon's voice played in open court and provided to the press in transcript form).

282. In his dissent in *Reed*, Justice Thomas suggested that technology might be deployed to protect the privacy interests of petition signers while still ensuring the integrity of submitted petitions. Doe v. Reed, 130 S.Ct. 2811, 2840–41 (2010) (Thomas, J., dissenting). However, his solutions did not include using technology to enhance public oversight that would allow citizens to access the signatures. He instead suggested that technology might be used to help the *Secretary of State* better vet petitions. *See id.* ("Washington . . . could put the names and addresses of referendum signers into a[n] . . . electronic database that state employees could search *without* subjecting the name and address of each signer to wholesale public disclosure. The secretary could electronically cross-reference the referendum database against the 'statewide voter registration list' contained in Washington's 'statewide voter registration database' . . . to ensure that each referendum signer meets Washington's residency and voter registration requirements. . . . An electronic referendum database would also enable the secretary to determine whether multiple entries correspond to a single registered voter, thereby detecting whether a voter had signed the petition more than once."). Thomas also suggested a system by which individual voters could log onto a website, enter a unique identifier, and confirm that his or her own name had not been fraudulently signed. *Id.* at 2841. As for citizen oversight, Thomas was satisfied with Washington's system for allowing two observers for each side to look on during the Secretary of State's verification process "so long as they make no record of the names, addresses, or other information on the petitions or related records." *Id.*

283. A cynic might point out that anyone could go to such a kiosk and simply copy out the names and addresses by hand, digitize the information, and spread signers' names far and wide. This is undoubtedly true. And that may happen. However, making it harder to access petition signatures online will result in this happening less, and only with great effort and expense. The hope is that by instituting systems that at least make it harder to let the toothpaste out of the tube in the first place, some degree of political obscurity may be maintained.

indicate their preference to share their name publicly when signing. Petitions could include a box giving signers the option to have a public listing of just their first name and last initial. For oversight purposes, those who require access to the full set of signatures and identifying information would still have access, but would be required to expend effort and would encounter speed bumps (as well as oversight-enhancing tools) using the mechanisms described above.

Finally, state agencies responsible for processing petition signatures might also consider disaggregating the privacy rights of petition signers depending on the type of petition at issue. There is an argument, for example, that recall petitions might implicate privacy interests of petition signers more than, say, candidate ballot access petitions, particularly in small jurisdictions. Perhaps state administrators might consider California-level restrictions appropriate for such petitions. The 2012 Wisconsin recall effort provides fodder for the idea. Rumors of petition fraud in the attempted 2012 recall of Wisconsin Governor Scott Walker were so widespread that the Wisconsin Government Accountability Board (WGAB) undertook the innovative strategy of live-streaming the signature validation process on its website to allow members of the public to watch online.[284] In addition, the WGAB voted to make the petitions available online, creating a website at which members of the public could view the scanned petition pages and search for petition signers by name.[285] The website did not allow members of the public to search by address. According to the website, "[t]he petitions are not address-searchable because addresses were not data-entered due to time and cost considerations."[286] Whether due to cost considerations or not, the inability to search by locality protected a measure of signers' political obscurity.

The idea of posting the signatures online met great criticism from advocacy groups concerned about the privacy of certain individuals, for example victims of domestic violence whose names and addresses would be exposed as a result of online release.[287] After weighing these concerns, the WGAB director and general counsel decided to release the signatures online nevertheless. The director emphasized the public nature of petition signing, explaining that, "[f]ew processes in the electoral system or elsewhere are more public than the signing of recall petitions against state-elected officials . . . . Petition signers chose to participate in the public process of initiating a recall election of the governor as well as other officeholders."[288] Not surprisingly, given the fervor surrounding the recall effort, the website was immediately swamped.[289] It seems likely that many, if not most, viewed the site to

284. *Recall Election Information*, WISC. GOV'T ACCOUNTABILITY BD., http://gab.wi.gov/elections-voting/recall (last visited Feb. 25, 2013).

285. *2012 Recall Petitions and Challenges*, WISC. GOV'T ACCOUNTABILITY BD., http://gab.wi.gov/elections-voting/recall/petitions (last visited Feb. 25, 2013); *Recall*, WISC. GOV'T ACCOUNTABILITY BD., https://webapps.wi.gov/sites/recall/default.aspx (last visited Feb. 25, 2013).

286. *2012 Recall Petitions and Challenges*, *supra* note 285.

287. *See* Clay Barbour, *GAB Posts Petitions Online: The Move Comes Despite Concerns that Residents Who Were Victims of Abuse or Assault May Be Put in Danger*, WIS. ST. J., Feb. 1, 2012, at A1 (discussing how making names and addresses of those who signed the petition unconditionally available to the public could create problems for victims of sexual or physical abuse).

288. *Id.* (quoting Kevin Kennedy, WGAB director and general counsel).

289. Mary Spicuzza, *Website of Signatures Swamped: The Searchable Database of Recall Petition*

satisfy curiosity about who opposed Walker rather than to detect fraud. But even if you believe the motivations were purely oversight driven, Wisconsin citizens will now likely think twice about signing recall petitions. This potential chill might have been avoided had Wisconsin thought through how it might have achieved its transparency and oversight goals without compromising political obscurity.

VI. CONCLUSION

The problem of waning political obscurity is particularly acute in an area lurking in the background of this Article: campaign finance disclosure. In a world in which anyone interested can very often find the name, political affiliation, address, occupation, and dollar amount of political contributions,[290] the question of political obscurity is particularly resonant. Will potential donors—at least those who do not have the resources to create anonymous donation mechanisms—refrain from contributing if political obscurity is lost? Some research suggests the answer is yes.[291] One common observation is that the system is backward. Small donors are forced to reveal detailed personal information while larger donors—whose identities arguably offer more salient political information—are able to mask their identity.[292] A suggested fix is to increase minimum dollar reporting requirements so that nominal political contributions remain anonymous.[293] Bruce Cain intelligently suggests partial disclosure for small contributors—for example, occupation and amount, but not name and address.[294]

In a sense, small political donors and petition signers share much in common. Both function essentially as "drops in the bucket" in terms of political impact. And, in

Signers is Overwhelmed Minutes After it's Rolled Out, WIS. ST. J., Mar. 9, 2012, at A3.

290. *See, e.g.*, *Campaign Finance Disclosure Portal*, FED. ELECTION COMMISSION, http://fec.gov/pindex.shtml (last visited Feb. 25, 2013) (allowing users to see what political candidates people are financially supporting); *HuffPost Fundrace*, HUFFINGTON POST, http://www.huffingtonpost.com /news/huffpost-fundrace (last visited Feb. 25, 2013) (allowing users to search for individual donors by name, employer, or zip code); OPENSECRETS.ORG, http://www.opensecrets.org (last visited Feb. 25, 2013) (keeping track of the amount of money spent on campaigns).

291. *See, e.g.*, Raymond J. La Raja, Political Participation and Civic Courage: The Negative Effect of Transparency on Making Campaign Contributions 1 (November 29, 2012) (unpublished paper), *available at* http://ssrn.com/abstract=2202405 (finding that political donors, "refrain from making contributions or reduce their donations to avoid disclosing their identities").

292. *See, e.g.*, Richard Briffault, *Campaign Finance Disclosure 2.0*, 9 ELECTION L.J. 273, 286 (2010) (arguing that large donors no longer worry about disclosing their donations); Richard L. Hasen, *Chill Out: A Qualified Defense of Campaign Finance Disclosure Laws in the Internet Age*, 27 J.L. & POL. 557, 568–70 (2012) (arguing that the amount of money in the system could cause quid pro quo corruption making it necessary to have disclosure laws); Lloyd Hitoshi Mayer, *Disclosures About Disclosure*, 44. IND. L. REV 255, 280 (2010) (arguing for changes in current disclosure system to prevent retaliation against donors); McGeveran, *supra* note 28, at 859–60 (stating the Supreme Court has found no problems with disclosure of modest campaign contributions).

293. Mayer, *supra* note 292, at 282–83; *see also* Spencer Overton, *The Participation Interest*, 100 GEO. L. J. 1259, 1300–01 (2012) (arguing that campaign contributions of less than $500 be exempt from disclosure).

294. *See* Bruce Cain, *Shade from the Glare: The Case for Semi-Disclosure*, CATO UNBOUND (Nov. 8, 2010, 11:08 AM), http://www.cato-unbound.org/2010/11/08/bruce-cain/shade-from-the-glare-the-case-for-semi-disclosure/ (noting that there is value in knowing from where a candidate receives money, but no informational gain in knowing a specific donor's name).

both cases the state has an interest in encouraging participation; democracy is improved the more citizens take part.[295] But potential solutions in the political contribution context are not transferable to the petition signature context. Verifying the identity and validity of all signers is a core purpose of transparency. And, there are no varying degrees of signing around which to build thresholds—a person has either signed or has not. But the impulse to protect small donors is the same as the impulse to protect petition signers: to maintain political obscurity in order to encourage, or at least not hamper, political participation.

Because of the absence of a threshold-based solution, the fix in the petition context must be more nuanced. First, courts, legislators, and state administrators must acknowledge the value of political obscurity, its fragility in the modern day, and the consequences of the state's role in diminishing it. Doing so may enable courts to move beyond outdated distinctions between "public" and "private," and do away with a decades-old harassment formula that fails to acknowledge the real harm at hand. Confronting the need to maintain a degree of political obscurity will also force those who administer petitions to rethink processes in place and develop methods to respect important political privacy rights of petition signers.

One might argue that such efforts are not worth the bother. As political campaigns and other private actors engage in massive voter preference cataloguing, there is an argument that petition signature data is spit in the sea of information being gathered about individual voter preferences. But, as political data gatherers are increasingly recognizing, petition data is a higher value target than the car one drives or the beer one drinks.[296] States that record petition-signing activities in their publicly accessible voter registration databases or affirmatively post petition signatures online in searchable format are facilitating exposure in a way not dissimilar to exposing the content of voters' ballots. As custodians of official petitions, states must begin to think more creatively about how to protect political obscurity while maintaining a transparent petitioning process.

295. *See* Overton, *supra* note 293, at 1273–88 ("Participation exposes the electorate to a variety of ideas and viewpoints, furthers self-government, and enhances the legitimacy of government decisions."); *see also* McGeveran, *supra* note 28, at 880 (addressing costs and benefits of disclosure regimes).

296. Charles Duhigg, *Campaigns Mine Personal Lives to Get out the Vote*, N.Y. TIMES, Oct. 14, 2012, at A1.