Florida State University Law Review

Volume 48 | Issue 4 Article 6

Summer 2021

Privacy's "Three Mile Island" and the Need to Protect Political Privacy in Private-Law Contexts

Raymond H. Brescia
Albany Law School

PRIVACY'S "THREE MILE ISLAND" AND THE NEED TO PROTECT POLITICAL PRIVACY IN PRIVATE-LAW CONTEXTS

RAYMOND H. BRESCIA*

ABSTRACT

When it was revealed that Cambridge Analytica obtained the personal and private information of eighty-seven million Facebook users to aid the 2016 U.S. presidential campaign of Donald J. Trump, it was described as privacy's "Three Mile Island": an event, like the famed nuclear accident from which the term comes, that would shake and shape an industry and its approach to digital privacy and the underlying political information such privacy protects. In the intervening four years, despite these revelations, while some social media companies took voluntary measures to prevent a repeat of the types of abuses that plagued the 2016 election, little has changed in terms of the legal infrastructure that could protect the type of private information essential to the functioning of democracies. But what the Cambridge Analytica scandal also made clear is that threats to private information revealed and embedded in our digital activities threaten democracy. What is more, these threats risk undermining individual identity and autonomy and the ability of individuals to pursue individual and collective self-determination. An individual's political identity—with whom she associates, what she says, what she thinks, the questions and ideas she explores, for whom she votes—is all caught up in notions of political privacy. While current public-law protections are fairly robust when it comes to protecting political privacy, even as some fear that current responses to the pandemic may require a degree of intrusion upon privacy by government, the threats to privacy that have emerged in the digital age preceded the current public health crisis and emanate mostly from private actors, where protections for political privacy are quite weak. Nevertheless, democracy requires a high degree of protection for individual identity and political privacy, regardless of the source of the threat, especially when the lines between private action and public effects are blurred, as in the Cambridge Analytica scandal. Given the importance of the integrity of identity to democracy and the fact that many of the threats to political privacy emanate from private actors, as this Article shows, enhanced protections for this political privacy are also necessary in the private-law context. Calls for greater protection of digital privacy often result in recommendations that a single institution—the market, political bodies, or the courts—should take a greater role in policing online privacy. Yet these institutions are often interdependent when it comes to protecting digital privacy, and, by extension, political privacy.

* Hon. Harold R. Tyler Chair in Law & Technology and Professor of Law, Albany Law School.

Efforts promoted through one institution can often have positive—and negative—spillover effects on the functioning of other institutions: they can at times strengthen the protections of such privacy in other institutional settings or undermine the ability of those other institutions to function effectively to protect political privacy. So which institution or set of institutions is best suited to protect such political privacy? This question calls for the application of the method known as comparative institutional analysis, which assesses the relative strengths and weaknesses of different institutions in achieving desired policy goals. At the same time, as this discussion will reveal, even comparative institutional analysis, if it does not take into account the extent to which different institutional settings can have spillover effects on the ability of other institutions to achieve particular policy goals, fails to offer sufficient tools for the assessment of the best institution or institutions to achieve such goals. Indeed, as this Article attempts to show, at least when it comes to protecting political privacy in private-law contexts, any effective institutional response to the threats to political privacy will likely require not just an appreciation for the ways in which different institutional settings are interdependent when it comes to achieving that goal but also that any such effort will require an integrated and comprehensive approach that spans different institutional settings. In the end, this Article is an attempt to use the tools of comparative institutional analysis to assess the relative abilities of different institutions to protect political privacy, including an assessment of the litigation that has arisen in the wake of the Cambridge Analytica scandal, to determine the role of different institutions in protecting political privacy in private-law—as opposed to public-law—settings. Through a review of this and other litigation to protect digital privacy, which, more and more, affects political privacy, I will show not just how different institutional settings can strengthen the functioning of other settings but also how they can undermine such settings. Thus, given the fact that institutions that protect political privacy can often work at cross-purposes in policing political privacy, this Article argues for the need for comprehensive, integrated, and cooperative action across institutions to ensure the proper protection of this type of privacy.

INTRODUCTION

In the early spring of 1979, a reactor core at the nuclear power plant located on Three Mile Island, just south of Harrisburg, Pennsylvania, had a partial failure, resulting in the release of radioactive material

into the surrounding atmosphere.[1] While the community surrounding the reactor largely avoided the most severe potential health risks of that release, the nuclear industry in the United States suffered a severe backlash, and calls for reform were common.[2] After the Three Mile Island crisis, the cost of the manufacture of and the approval process for building a new nuclear reactor, which had already begun to rise, became far more expensive.[3] Between the disaster and 2012, not a single nuclear reactor was approved for construction by the U.S. Nuclear Regulatory Commission.[4] In the wake of the disaster, many in the public feared the risks of nuclear power, despite some of its environmental benefits, and regulators and elected officials responded to such fears, not only making it more difficult to construct new plants but also—appropriately—shoring up oversight of existing and operating plants.[5] As a result of the public knowledge of and concern over the safety of nuclear power and governmental attention to oversight of the industry in response, the U.S. has not faced a similar nuclear disaster in the more than four decades since the Three Mile Island incident.[6]

Fast-forward to early 2017, long after the final tally of ballots for the U.S. presidential election of 2016. It was then that revelations emerged that a group based in the United Kingdom, Cambridge Analytica, had access to and used the private information of over 87 million Facebook users to aid the victorious presidential campaign of Donald J. Trump.[7] Cambridge Analytica and, by extension, the Trump campaign, obtained this information in a clandestine way, and it became

1. Elana Glowatz, *Three Mile Island Accident Deaths, Location: Facts on Nuclear Meltdown's Anniversary*, NEWSWEEK (Mar. 28, 2018, 12:31 PM), https://www.newsweek.com/three-mile-island-accident-deaths-location-facts-nuclear-meltdown-anniversary-864161[https://perma.cc/MQ6Z-C8Z9].

2. *See generally* The Learning Network, *March 28, 1979 | Nuclear Accident Occurs at Three Mile Island Plant*, N.Y. TIMES: THE LEARNING NETWORK (Mar. 28, 2012, 4:02 AM), https://learning.blogs.nytimes.com/2012/03/28/march-28-1979-nuclear-accident-occurs-at-three-mile-island-plant/?searchResultPosition=1[https://perma.cc/99GP-MNUX]; *see also* Peter Behr, *Three Mile Island Still Haunts U.S. Nuclear Industry*, N.Y. TIMES (Mar. 27, 2009 https://archive.nytimes.com/www.nytimes.com/gwire/2009/03/27/27greenwire-three-mile-island-still-haunts-us-reactor-indu-10327.html [https://perma.cc/H2SM-WUFK].

3. Nathan Hultman & Jonathan Koomey, *Three Mile Island: The Driver of US Nuclear Power's Decline?*, 69 BULL. ATOMIC SCIENTISTS 63, 64-65 (2013).

4. Ayesha Rascoe, *NRC Approves First New Nuclear Plant in a Generation*, REUTERS (Feb. 9, 2012, 12:15 PM), https://www.reuters.com/article/us-usa-nuclear-license/nrc-approves-first-new-nuclear-plant-in-a-generation-idUSTRE8181T420120209 [https://perma.cc/PM4X-Y8HG].

5. Neal H. Lewis, *Interpreting the Oracle: Licensing Modification, Economics, Safety, Politics, and the Future of Nuclear Power in the United States*, 16 ALB. L.J. SCI. & TECH. 27, 55 (2006).

6. *Id.* at 55-58.

7. Paul Lewis & Paul Hilder, *Leaked: Cambridge Analytica's Blueprint for Trump Victory*, THE GUARDIAN (Mar. 23, 2018, 8:53 AM), https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory [https://perma.cc/5VGZ-HSXX]; *see also* Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram*, VOX (May 2, 2018, 3:25 PM),

the basis for campaign advertisements and messaging to those users in ways that might encourage them to vote for Mr. Trump.[8] Cambridge Analytica gained access to this information from a researcher who had previously obtained permission from a relatively small number of Facebook users who had consented to allow that researcher to not just pry into their own private Facebook pages but also gain access to the members of these users' extended networks.[9] The revelations about this data breach served as a wakeup call to many who were unaware such private information was so permeable, that it could be made available to outside entities and individuals so easily.[10] Microsoft's general counsel, Brad Smith, has called the Cambridge Analytica scandal "the privacy equivalent of Three Mile Island," a moment of reckoning when society is supposed to wake up to the reality that the term "digital privacy" may be an oxymoron.[11] But for some, this was business as usual and came as no surprise. Even in the wake of the Cambridge Analytica scandal, little has changed in terms of protecting digital privacy. While the European Union and several U.S. jurisdictions have taken action to protect digital privacy, the main approach that many of these efforts espouse is enhanced disclosure regimes, not necessarily more robust accountability measures.[12] What is more, with the onset of the novel Coronavirus, it only appears that greater intrusion into digital privacy is likely, and some fear governments will not scale back such incursions when the current crisis passes.[13]

---

https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram [https://perma.cc/C63Q-JWSA].

8. Chang, *supra* note 7.

9. *Id.*

10. *See generally* Alex Hern, *Breach Leaves Facebook Users Wondering: How Safe is My Data?*, THE GUARDIAN (Mar. 18, 2018, 1:35 PM), https://www.theguardian.com/news/2018/mar/18/breach-leaves-facebook-users-left-wondering-how-safe-is-my-data[https://perma.cc/XGK4-LZW5].

11. BRAD SMITH & CAROL ANN BROWNE, TOOLS AND WEAPONS: THE PROMISE AND THE PERIL OF THE DIGITAL AGE 144 (2019); Andy Kroll, *We're Not Ready for a Massive Digital Terror Attack*, ROLLING STONE (Sept. 9, 2019, 1:32 PM), https://www.rollingstone.com/politics/politics-features/cambridge-analytica-christchurch-trump-snowden-brad-smith-881314/ [https://perma.cc/66GX-VJDM].

12. *See, e.g.*, Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 375-405 (2019) (describing approach of the European Union's new privacy regulations and their direct and indirect effects on U.S. law). *See also* Alfred Ng, *At Hearing on Federal Data-Privacy Law, Debate Flares Over State Rules*, CNET (Feb. 26, 2019, 10:52 AM), https://www.cnet.com/news/at-hearing-on-federal-data-privacy-law-debate-flares-over-state-rules/ [https://perma.cc/PC8G-VLPL] (describing Congressional hearings where witnesses and elected officials debated the proper role of state privacy regulations in relation to federal protections).

13. Iain Marlow, *Virus Hands World Leaders Sweeping Powers They May Never Give Up*, BLOOMBERG (Mar. 24, 2020, 8:42 AM), https://www.bloomberg.com/news/articles/2020-03-25/virus-gives-world-leaders-sweeping-powers-they-may-never-give-up [https://perma.cc/DDW4-DV89]. Another phenomenon of privacy implicated by the current pandemic relates to the potential intrusiveness of surveillance and its impact on issues of identity. As an example of some of the themes described throughout this Article, a recent

Nevertheless, the Cambridge Analytica scandal *has* resulted in regulators obtaining a $5 billion settlement with Facebook,[14] though even this has caused some to argue this is an insufficient penalty to deter Facebook and other social media companies from engaging in these sorts of activities in the future.[15] As the 2020 election is mostly in the rear-view mirror, and social media companies appeared to have done a better job, voluntarily, of trying to prevent election meddling, the legal infrastructure protecting political privacy in the digital world has not changed much since the Cambridge Analytica scandal broke.[16] While the U.S. Congress may ultimately step in to pass more robust protections (or may preempt stronger state-based rules), litigation is still working its way through the courts in which Facebook users are suing for damages against Facebook for the Cambridge Analytica breach.[17] This Article will analyze this litigation and other lawsuits like it involving digital privacy, particularly as they relate to what I call "political privacy."[18] I will ask whether such legal challenges are a viable means through which individuals whose digital privacy, as it relates to their political affairs, has been accessed and breached can seek meaningful redress.[19] But it will not solely look at the courts as an institution to protect political privacy; rather, it will assess the potential comparative role of the courts, in relation to other institutions, in protecting political privacy. Moreover, it will examine the extent to which these institutions are interdependent and must work collaboratively to accomplish the goal of protecting such privacy.

---

outbreak of COVID-19 in South Korea may be linked to several nightclubs, including those whose patronage is mostly LGBTQ individuals. Given societal stigma that still attaches in this culture to the LGBTQ community, there is fear that contact tracing will either "out" the members of the community or will keep some from coming forward to admit that they frequented such locations. Sangmi Cha & Josh Smith, *South Korea Tracks New Coronavirus Outbreak in Seoul Nightclubs*, U.S. NEWS (May 8, 2020), https://www.newsweek.com/new-cluster-coronavirus-infections-linked-nightclubs-south-korea-begins-reopen-1502769 [https://perma.cc/FD4A-UKDX].

14. Brian Fung, *Facebook Will Pay an Unprecedented $5 Billion Penalty Over Privacy Breaches*, CNN BUSINESS (July 25, 2019, 1:08 PM), https://www.cnn.com/2019/07/24/tech/facebook-ftc-settlement/index.html [https://perma.cc/V9CV-69GB].

15. *See, e.g.*, Kara Swisher, *Put Another Zero on Facebook's Fine. Then We Can Talk*, N.Y. TIMES (April 25, 2019), https://www.nytimes.com/2019/04/25/opinion/facebook-fine.html [https://perma.cc/L95G-KSPW] (describing the Facebook FTC fine as the equivalent of a "parking ticket" because of Facebook's revenue and market valuation).

16. For a discussion of social media companies' efforts to combat the spread of disinformation in the leadup to the 2020 election, see Kate Conger et al., *Twitter and Facebook Worked to Crack Down on Election Disinformation, but Challenges Loom*, N.Y. TIMES (Nov. 4, 2020), https://www.nytimes.com/2020/11/04/us/politics/twitter-and-facebook-worked-to-crack-down-on-election-disinformation-but-challenges-loom.html [https://perma.cc/79EV-ZNZ4].

17. *See infra* Part IV (describing Cambridge Analytica litigation).

18. *See infra* Part I (describing political privacy).

19. *See infra* Part IV.

To date, scholarship focused on digital privacy tends to highlight the need for new legislation or regulation,[20] new judicial remedies,[21] or more robust oversight by law enforcement authorities.[22] Because of this, it tends to fall into an approach sometimes labeled "single institutional analysis,"[23] which looks at the role of a particular institution in bringing about a desired policy outcome, as opposed to "comparative institutional analysis," which assesses the relative strengths and weaknesses of different institutions when compared against each other.[24] Through the tools of this type of comparative institutional analysis, this Article will use the Facebook litigation in the wake of the Cambridge Analytica scandal to assess the relative strengths of the different approaches to enhancing and protecting political privacy, addressing the proper role of different institutions—legislators, executive authorities, the market, and the courts—in preserving such privacy.[25] But even such comparative institutional analysis fails to recognize the ways that these different institutions are interdependent, and the history, to date, of regulating digital privacy has not come to grips with the fact that a weak institutional response from one sector can undermine even more robust institutional responses elsewhere. Instead, I will argue that a comprehensive, integrated, and multi-institutional approach is needed to enhance and secure political privacy.

With these goals in mind, this Article proceeds as follows: Part I describes what I call "political privacy," which is rooted in the integrity of one's identity. Part II describes the current threats to political privacy in the digital world, with a particular focus on the Cambridge Analytica scandal. In Part III, I will discuss the current state of privacy protections through the markets and the political process, using the tools of comparative institutional analysis[26] to do so. Part IV will explore litigation to challenge such threats, with a particular emphasis on the Cambridge Analytica scandal. In Part V, I will attempt to describe some of the components of an institutionally integrated regime

20. *See, e.g.*, Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1179-89 (2015) (describing need for the expansion of privacy regulations to protect certain types of vulnerable information); Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*, 10 CYBARIS INTELL. PROP. L. REV. 1, 30-40 (arguing for and describing components of a national data privacy law).

21. For example, Jack Balkin has proposed remedies, enforceable in tort, for breach by "information fiduciaries" of individual's private information. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205-09 (2016).

22. Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 749-54 (2016) (outlining role of state attorneys general in enforcing privacy protections).

23. *See* NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 6, 23 (1994) [hereinafter KOMESAR, IMPERFECT ALTERNATIVES].

24. *Id.* at 4-7.

25. *See id.* at 4-9.

26. *See infra* Part III.A. (describing comparative institutional analysis).

for the protection of political privacy in private-law contexts. This conclusion points not just to the need for this inter-institutional response but also reveals one facet of comparative institutional analysis itself—the notion that comparative institutional analysis must recognize the fact that institutions are not monolithic. In other words, institutions often share a degree of interdependence that does not always allow for the utilization of a traditional approach to comparative analysis: for example, one that tends not to take into account or consider this institutional interdependence.

I. POLITICAL PRIVACY

In a recent and pathbreaking work, Danielle Citron describes the importance of sexual privacy to autonomy and human flourishing.[27] For Citron, "[s]exual privacy concerns the social norms governing the management of boundaries around intimate life"[28] and "[i]nvolves the extent to which others have access to and information about people's naked bodies (notably the parts of the body associated with sex and gender); their sexual desires, fantasies, and thoughts;"[29] their "communications related to their sex, sexuality, and gender;"[30] and related "intimate activities."[31] It is critical to protect sexual privacy because it is so essential to human flourishing: indeed, for Citron, it is "foundational for the exercise of human agency and sexual autonomy"[32] and "enables individuals to set the boundaries of their intimate lives."[33] Unwanted exposure of one's most intimate details can impact "a person's life plans,"[34] and thus, "[s]exual privacy therefore creates a space for individuals to figure out their *future selves*."[35] Sexual privacy is also critical to "fostering intimacy" and "combating subordination,"[36] as "sexual-privacy invasions"[37] have a "disproportionate impact . . . on women, sexual minorities, and nonwhites, and on the lived experiences and suffering of these marginalized communities."[38] Thus, to summarize, for Citron, sexual privacy not only promotes autonomy and self-determination, it also helps to combat subordination. As the following discussion shows, political privacy accomplishes many of the same things and holds a critical place in the functioning of democracies.

27. Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1870 (2019).
28. *Id.* at 1880.
29. *Id.*
30. *Id.*
31. *Id.*
32. *Id.* at 1882.
33. *Id.*
34. *Id.* at 1884.
35. *Id.* (footnote omitted).
36. *Id.* at 1888, 1890.
37. *Id.* at 1891.
38. *Id.*

A. *Political Autonomy and Privacy in Democracies*

Privacy protections that preserve the ability of the individual to act in the world to realize self-determination, both individually and collectively, are critical to democracy.[39] Respect for the individual is at the center of this understanding of liberal democracy, and that respect translates into a recognition that individuals should play a part in the deliberations that generate the policies and laws that govern society.[40] Robert Post calls the ideal of autonomy "foundational for the democratic project,"[41] and autonomy is needed in the political realm to come to decisions with a degree of independence. [42] This autonomy is closely connected to self-government, and being autonomous means "being or doing only what one freely, independently, and authentically chooses to be or do."[43]

This autonomy begins with identity formation.[44] This identity is not just a function of how we might see ourselves in the world. We also find communion with others and "come out" as embracing a particular public identity or identities when we engage in democratic practices.[45] Preserving the protection of individual identity should be a centerpiece of the democratic endeavor[46] because at the heart of the practice of self-

39. Frank I. Michelman, *Law's Republic*, 97 YALE L.J. 1493, 1533-37 (1988) [hereinafter Michelman, *Law's Republic*] (emphasizing the importance of privacy rights in securing political autonomy and democracy).

40. C. Edwin Baker, *Counting Preferences in Collective Choice Situations*, 25 UCLA L. REV. 381, 414 (1978) (arguing that mutual respect—between the individual and the community—is critical for functioning societies). *See also* Philip Pettit, *Democracy, Electoral and Contestatory*, 42 NOMOS: AM. SOC'Y FOR POL. & LEGAL PHIL. 105, 106 (2000) [hereinafter NOMOS XLII] (arguing that in a democracy, "the governed people enjoy control over the governing authorities").

41. Robert Post, *Meiklejohn's Mistake: Individual Autonomy and the Reform of Public Discourse*, 64 U. COLO. L. REV. 1109, 1123 (1993) (footnote omitted).

42. *See* CASS R. SUNSTEIN, THE PARTIAL CONSTITUTION 177 (1993) (arguing one of the fundamental goals in a democracy is "protecting free processes of preference formation").

43. John Christman, *Feminism and Autonomy*, *in* "NAGGING" QUESTIONS: FEMINIST ETHICS IN EVERYDAY LIFE 17, 18 (Dana Bushnell ed., 1995). *See also* Robert Post, *Participatory Democracy and Free Speech*, 97 VA. L. REV. 477, 487-88 (2011) (describing the relationship between First Amendment jurisprudence and opinion formation, autonomy, and self-government).

44. *See, e.g.*, Robert Post, *Democracy, Popular Sovereignty, and Judicial Review*, 86 CALIF. L. REV. 429, 439 (1998) (arguing "democracy depends upon a social structure that sustains and nourishes the value of collective self-determination as constitutive of collective and individual identity") (footnote omitted).

45. *See, e.g.*, Monica Anderson & Skye Toor, *How Social Media Users Have Discussed Sexual Harassment Since #MeToo Went Viral*, PEW RESEARCH CENTER: FACT TANK (Oct. 11, 2018), https://www.pewresearch.org/fact-tank/2018/10/11/how-social-media-users-have-discussed-sexual-harassment-since-metoo-went-viral [https://perma.cc/YEN5-FDUA] (describing emergence of the #MeToo movement on social media that provided a platform and channel for survivors of sexual harassment to self-identify as such and seek solidarity with others).

46. *See, e.g.*, Anne C. Dailey, *Cultivating Feminist Critical Inquiry*, 12 COLUM. J. GENDER & L. 486, 487-89 (2003) (arguing that democratic institutions promote critical dissent in diverse institutions where individuals can identify with others who share common interests, backgrounds, and identities).

determination is the realization of individual and collective identity.[47] While the protection of this identity, this political identity, has *intrinsic* value as an aspect of the privacy right itself,[48] it also has an *instrumental* value, primarily because it enables individual autonomy and identity to be multiplied through collective action which catalyzes the pursuit of collective self-determination and through which social change comes about, as the following discussion shows.

B. The Instrumental Value of Collective Identity

A form of individual self-determination is reached through the pursuit of collective self-determination: when the individual seeks fellowship and opportunities to collaborate with others in order to bring about social change, to strive to mold society in ways that, to the greatest extent possible, reflect the wishes and desires of that individual and the others with whom she associates.[49] Legal theory has begun to embrace the connection between legal change and these acts of collective self-determination which occur, on a large scale, through these associations of individuals; that is, through the social movements they constitute.[50]

Moreover, in the field of social movement theory, there is a deep appreciation for the role of individual identity in social movement mobilization.[51] And individual identity is closely associated with collective

47. On the relationship between self-determination and liberal democracy, see Daniel Philpott, *In Defense of Self-Determination*, 105 ETHICS 352, 355-58 (1995).

48. Charles Fried, *Privacy*, 77 YALE L.J. 475, 476-78 (1968) (arguing for privacy's intrinsic value).

49. As Yuval Noah Harari writes, this capacity to cooperate is what sets human existence apart from other beings on the planet. YUVAL NOAH HARARI, SAPIENS: A BRIEF HISTORY OF HUMANKIND 25 (2015).

50. *See generally* DAVID COLE, ENGINES OF LIBERTY: HOW CITIZEN MOVEMENTS SUCCEED (2017); *see generally* LESLIE R. CRUTCHFIELD, HOW CHANGE HAPPENS: WHY SOME SOCIAL MOVEMENTS SUCCEED WHILE OTHERS DON'T (2018) (describing impact of social movements on legal doctrine in several contexts); Jack M. Balkin & Reva B. Siegel, *Principles, Practices, and Social Movements*, 154 U. PA. L. REV. 927, 929 (2006) (describing the role of social movements in changing legal culture); Scott L. Cummings, *The Social Movement Turn in Law*, 43 L. & SOC. INQ. 360, 360 (2018) (describing the embrace by legal scholars of an appreciation for the role of social movements in bringing about social change).

51. Some social movement theorists who espouse the rational actor model are often associated with the Resource Mobilization school, which believes the task of social movement leaders is to appeal to the sense that individuals may possess, as rational, calculative actors, that the benefits of participation in a movement outweigh the costs. *See, e.g.*, John D. McCarthy & Mayer N. Zald, *Resource Mobilization and Social Movements: A Partial Theory*, 82 AM. J. SOCIO. 1212, 1216-17 (1977) (describing the Resource Mobilization perspective). More recent social movement theories embrace the notion that individuals are often motivated by feelings of identity and solidarity and their decision to engage or not engage with a movement is a function of the affinity they feel for the members associated with it. *See, e.g.*, Pamela E. Oliver & Gerald Marwell, *Mobilizing Technologies For Collective Action*, *in* FRONTIERS OF SOCIAL MOVEMENT THEORY 251, 252 n.1 (Aldon D. Morris & Carol McClurg Mueller eds., 1992) (discussing role of identity in social movements); Steven M. Buechler, *Beyond Resource Mobilization? Emerging Trends in Social Movement Theory*, 34 SOCIO. Q. 217, 228-31 (1993) (describing role of identity, ideology, and culture in social movements).

identity, which has been described as the "shared definition of a group that derives from members' common interests, experiences, and solidarity."[52] Such shared identity helps to serve as a lens through which to see injustice in the world and seek to change it.[53] Such a shared identity serves a symbolic function, as a means of seeing not just oneself as part of a group, but also as a way to make sense of the world and a vehicle to try to change it.[54] Those that share this identity or identities come to believe there is something wrong in the world that needs remedying, and these injustices and the responses that might address them are seen through the prism of the identity or identities the group shares.[55] Alberto Melucci argues that collective identity emerges from the formation of "cognitive frameworks concerning the ends, means, and field of action"; the activation of "relationships between the actors, who interact, communicate, influence each other, negotiate, and make decisions"; and the making of "emotional investments, which enable individuals to recognize themselves."[56] For Steven Buechler, collective identities serve as both "essential outcomes of the mobilization process and crucial prerequisites to movement success."[57] What is more, the collective identity that emerges in and from a social movement organization "is a shorthand designation announcing a status—a set of attitudes, commitments, and rules for behavior—that those who assume the identity can be expected to subscribe to."[58] Such an identity is both "a public pronouncement of status" and an individual's "announcement of affiliation, of connection with others."[59] For Friedman and McAdam, "[t]o partake of a collective identity is to reconstitute the individual self around a new and valued identity."[60]

---

52. Verta Taylor & Nancy E. Whittier, *Collective Identity in Social Movement Communities: Lesbian Feminist Mobilization*, *in* FRONTIERS IN SOCIAL MOVEMENT THEORY 104, 104 (Aldon D. Morris & Carol McClurg Mueller eds., 1992).

53. *Id.* David A. Snow & Robert D. Benford, *Master Frames and Cycles of Protest*, *in* FRONTIERS IN SOCIAL MOVEMENT THEORY 133, 137 (Aldon D. Morris and Carol McClurg Mueller eds., 1992) (describing the role of collective identity in serving to generate "collective action frames" that help groups by "making diagnostic and prognostic attributions") (citation omitted).

54. Buechler, *supra* note 51, at 228 (describing the symbolic role of collective identity in social movements).

55. Judith M. Gerson & Kathy Peiss, *Boundaries, Negotiations, Consciousness: Reconceptualizing Gender Relations*, 32 SOC. PROBS. 317, 324 (1984) (describing relationship between collective identities and social mobilization).

56. Alberto Melucci, *Getting Involved: Identity and Mobilization in Social Movements*, *in* 1 INTERNATIONAL SOCIAL MOVEMENT RESEARCH: FROM STRUCTURE TO ACTION: COMPARING SOCIAL MOVEMENT RESEARCH ACROSS CULTURES 329, 343 (Bert Klandermans et al. eds., 1988).

57. Buechler, *supra* note 51, at 228.

58. Debra Friedman & Doug McAdam, *Collective Identity and Activism: Networks, Choices, and the Life of a Social Movement*, *in* FRONTIERS IN SOCIAL MOVEMENT THEORY 156, 157 (Aldon D. Morris & Carol McClurg Mueller eds., 1992).

59. *Id.*

60. *Id.*

And it is through this new and valued identity that social movements are formed that bring about social change, particularly for marginalized groups.[61]

Like with sexual privacy, political activities that operate through associational affiliations also bring about a sort of intimacy, a form of trust that breeds cooperation and a cooperation that breeds further trust between and among individuals and the social networks of which they are a part.[62] This is often referred to as a person's social capital, and can be viewed as networked trust; it is manifest in "networks of civic engagement [which] foster sturdy norms of generalized reciprocity and encourage the emergence of social trust."[63] As one example of the instrumental value of social capital specifically (to add to the instrumental value of political privacy as a whole), the presence of social capital in a community has proven to have significant spillover effects on community life, including improved economic performance in communities and nations where social capital is high,[64] and the functioning of government.[65]

In sum, individual and collective identities become springboards for collective action and are at the center of social movement activities and success; true individual and collective self-determination is realized and becomes a font of social change and social justice, particularly for marginalized communities.[66] At the same time, such identities may be under threat when so much of these identities are now reflected in our online activities.

C. *Threats to Digital Privacy Generally*

First and foremost, the digital self is now public. If one uses the internet and social media, a wide range of one's digital activities are

61. *See, e.g.*, William N. Eskridge, *Channeling: Identity-Based Social Movements and Public Law*, 150 U. PA. L. REV. 419, 425-442 (2001) [hereinafter Eskridge, *Channeling*] (describing the emergence of identity-based social movements in the late 20th century).

62. On the ways in which trust breeds cooperation and cooperation breeds trust, see John Brehm & Wendy Rahn, *Individual-Level Evidence for the Causes and Consequences of Social Capital*, 41 AM. J. POL. SCI. 999, 1001-02 (1997).

63. Robert D. Putnam, *Bowling Alone: America's Declining Social Capital*, 6 J. DEMOCRACY 65, 67 (1995) [hereinafter, Putnam, *Declining Social Capital*].

64. Stephen Knack & Philip Keefer, *Does Social Capital Have an Economic Payoff? A Cross-Country Investigation*, 112 Q. J. ECON. 1251, 1275-77 (1997).

65. *See* ROBERT D. PUTNAM ET AL., MAKING DEMOCRACY WORK: CIVIC TRADITIONS IN MODERN ITALY 121-51 (1993) (studying legacy of social capital in Italy to show regions with higher levels of social capital had better functioning governments); *see also* Stephen Knack, *Social Capital and the Quality of Government: Evidence from the States*, 46 AM. J. POL. SCI. 772, 772 (2002) (engaging in comparative analysis of levels of social capital in U.S. states to show correlation between levels of social capital and effective functioning of government).

66. *See* Eskridge, *Channeling*, *supra* note 61, at 425-42 (describing identity-based social movements in the late twentieth century).

subject to exposure. In authoritarian regimes, this comes as no surprise.[67] But this is also occurring in democratic societies, including the United States. The main culprits are the private companies that offer web and mobile services, often through so-called browser extensions and plug-ins to popular search engines like Chrome, the search engine of Google.[68] Amazon also tracks user activities on its site, but mostly for its own purposes.[69] Facebook has long marketed itself as having a wide range of information on its users' preferences and interests, with advertising to its users based on such information as the main source of Facebook's revenue.[70] As is becoming apparent, a broad range of personal information is available for sale to marketers and other companies, and this is all "legal" in the sense that users tend to give consent to sites and applications that allow them to harvest and sell their personal data.[71] It is certainly the case that data breaches, which seem to be occurring with greater frequency, expose a great deal of private information when they occur; the reality is, however, much of this information is available, now, for sale to anyone who will pay for it.[72] Indeed, activities like browser histories and searches, medical records, tax filings, and other highly personal information are often available for sale to companies seeking it.[73] There is thus a near parallel uni verse, an "upside down" as I have called it,[74] in which our very private information follows us as we move through the digital world and is open for viewing, sale, and use.[75]

---

67. *See* ZEYNEP TUFEKCI, TWITTER AND TEAR GAS: THE POWER AND FRAGILITY OF NETWORKED PROTEST 223-61 (2016) (describing government censorship of contemporary social movements).

68. Geoffrey A. Fowler, *I Found Your Data. It's for Sale*, WASH. POST (July 18, 2019, 8:00 AM) https://www.washingtonpost.com/technology/2019/07/18/i-found-your-data-its-sale/ [https://perma.cc/333S-MRQE] (describing tracking of digital activities through plugins).

69. *Id.* (noting that Amazon's information about users stays within the company).

70. ROGER MCNAMEE, ZUCKED: WAKING UP TO THE FACEBOOK CATASTROPHE, 189-91 (2019) (describing Facebook's business model and its susceptibility to exploitation from third parties).

71. *See* discussion *infra* Part IV.B.

72. *See* McNamee, *supra* note 70, at 190-91 (detailing availability of user data of digital companies for purchase by third parties).

73. Fowler, *supra* note 68 (describing user information that is available for purchase by third parties).

74. *See* Raymond H. Brescia, *Zoning Cyberspace: Protecting Privacy in the Digital Upside Down*, 5 UTAH L. REV. 1219, 1223 (2021) [hereinafter Brescia, *Zoning Cyberspace*] (referencing the "upside down" in the Netflix Original Series *Stranger Things*, which is described as a terrifying parallel universe that mimics the real world); *see also* Brian Barth, *Big Tech's Big Defector*, THE NEW YORKER (Nov. 25, 2019), https://www.newyorker.com/magazine/2019/12/02/big-techs-big-defector [https://perma.cc/V8S9-PE7G] (quoting venture capitalist Roger McNamee as saying technology companies create "data voodoo dolls" of individuals based on their online activities).

75. *See* Brian X. Chen, *'Fingerprinting' to Track Us Online Is on the Rise. Here's What to Do*, N.Y. TIMES (July 3, 2019), https://www.nytimes.com/2019/07/03/technology/personaltech/fingerprinting-track-devices-what-to-do.html [https://perma.cc/F2LN-72JA] (describing tracking software that follows unique individuals' digital activities).

We might see at least some of the use of this information as completely harmless: we may not care if a company uses it to try to convince us to purchase a different brand of fabric softener. But when such information is used to impact, even manipulate, our political choices, and when our knowledge that our personal political information may be exposed, which may chill our willingness to engage in acts that reveal such information, the transparency of our political identity has significant downstream effects. Indeed, in these ways, threats to digital privacy undermine the integrity of our political identities. And when an individual does not have this integrity of identity, this political privacy, she is not able to think independently, explore information freely to help form an opinion on matters, or collaborate with other like-minded people to shape society as she wishes in the pursuit of self-determination. This has an intrinsic cost, as the individual's privacy has value in itself, but it also has instrumental effects: namely, reducing the ability of the individual to associate with others, chilling expressive speech and action, and impairing the process by which social change comes about and the collective goods such social change generates.[76] Thus, threats to privacy, grounded in a disregard for individual and collective identity, undermine democracy and curtail the ability of individuals and groups to mobilize to pursue their collective rights, combat subordination, and further social change.[77] Thus, protections for our political identities, as they are manifest in our digital existence, are critical to democracy and self-determination. Given the importance of this form of privacy, what current protections exist for it in both the public- and private-law contexts? That question I take up next.

D. Existing Legal Protections for Political Privacy

Political privacy enables greater autonomy and promotes individual and collective self-determination, particularly for marginalized groups.[78] Digital platforms can play a significant role in fostering the exploration, creation, and maintenance of individual and collective

76. Scholarship on collective goods often fails to distinguish between and blends the concepts of "public goods" and "collective goods." For a discussion of collective goods and public goods that views them as mostly interchangeable, see PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 227-31 (1995). Some scholarship also focuses on what are called "club goods": the benefits that are derived from membership in a group. *See* RICHARD CORNES & TODD SANDLER, THE THEORY OF EXTERNALITIES, PUBLIC GOODS, AND CLUB GOODS 347-51 (2d ed. 1996). For a discussion of public goods, like civil rights, that are a product of collective action, see DENNIS CHONG, COLLECTIVE ACTION AND CIVIL RIGHTS 2-4 (1991).

77. Anil Kalhan, *The Fourth Amendment and Privacy Implications of Interior Immigration Enforcement*, 41 U.C. DAVIS L. REV. 1137, 1181-85 (2008) (describing structural harms, like threats to associational interests, associated with a loss of privacy).

78. *See generally* SARAH J. JACKSON ET AL., #HASHTAGACTIVISM: NETWORKS OF RACE AND GENDER JUSTICE (2020) (describing the role of social media in serving as an important platform for social justice on behalf of marginalized communities).

identity.[79] In public-law settings, there are strong protections for political privacy, whether it is through individual rights to free speech and freedom of religion, or collective rights, like the freedom of petition and assembly, which, collectively, have been read to create the freedom of association: that is, the freedom of individuals to come together collectively to promote social change.[80] But threats to political privacy, particularly as that privacy is valuable in the digital world, also emanate from actors not covered by the reach of public-law.[81] In the midst of a raging global pandemic, and people relying more and more on digital tools to communicate and coordinate, the freedom of such means of communication from surveillance—both public and private—is paramount to the ability of individuals to affect social change in an environment where social distancing is the norm.[82] And when threats to such efforts come from private actors outside the reach of public-law protections, it only heightens the need for the protection of political privacy in private-law contexts.[83] In order to protect political privacy in a world where much of our personal political information is maintained by private actors, we need some means to protect this information in private-law contexts.[84] In the next Part, I will discuss a range of the threats to political privacy in the digital world currently emanating from actors beyond the reach of domestic constitutional protections.

---

79. *See, e.g.*, JEREMY HEIMANS & HENRY TIMMS, NEW POWER HOW POWER WORKS IN OUR HYPERCONNECTED WORLD—AND HOW TO MAKE IT WORK FOR YOU 54-80 (2018) (describing methods for digitally enhanced social activism).

80. *See, e.g.*, Nat'l Ass'n for the Advancement of Colored People v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958) (recognizing the First Amendment right in associational privacy) [hereinafter NAACP v. Alabama]; *see generally* Anita L. Allen, *Associational Privacy and the First Amendment: NAACP v. Alabama, Privacy and Data Protection*, 1 ALA. C.R. & C.L.L. REV. 1 (2011) (describing the legacy of NAACP v. Alabama). *See also* William N. Eskridge, Jr., *Some Effects of Identity-Based Social Movements on Constitutional Law in the Twentieth Century*, 100 MICH. L. REV. 2062, 2335-36 (2002) (describing the Court's recognition of an associational right in NAACP v. Alabama); Frank H. Easterbrook, *Implicit and Explicit Rights of Association*, 10 HARV. J.L. & PUB. POL'Y 91, 94 (1987) (same).

81. On the origins of the "state action" doctrine which prohibits the application of many constitutional principles to private actors, see Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503, 507-19 (1985).

82. *See* Martin Austermuhle, *From Zoom to Facebook, the Pandemic Is Changing How People Engage With Their Local Government*, WAMU (Apr. 23, 2020), https://wamu.org/story/20/04/23/from-zoom-to-facebook-the-pandemic-is-changing-how-people-engage-with-their-local-government/ [https://perma.cc/PPP6-Q858].

83. And tech giants have also shown a willingness to utilize the information they have on those in their orbit to monitor their political activities, as it was revealed that Uber tracked the location of drivers on its network to monitor whether they participated in demonstrations in China to protest the ride-hailing company. Dante D'Orazio, *Uber is Tracking Its Drivers in China, Will Fire Anyone Attending Taxi Protests*, THE VERGE (June 14, 2015, 10:41 AM), https://www.theverge.com/2015/6/14/8778111/uber-threatens-to-fire-drivers-attending-protests-in-china [https://perma.cc/8G2C-TNBC].

84. Of course, the line between the public and the private in the context of digital privacy is extremely blurry. *See* Morton J. Horwitz, *The History of the Public/Private Distinction*, 130 U. PA. L. REV. 1423, 1425-28 (1982).

II. THREATS TO POLITICAL PRIVACY, AUTONOMY AND THE INTEGRITY OF POLITICAL IDENTITY IN THE DIGITAL WORLD

Again, the exposure of private information in the political sphere has significant intrinsic and instrumental negative effects—effects that go beyond whether some company might use this information to sell us its particular brand of grooming product. Intrusions upon the integrity of our political identities can inhibit our political development and chill our political activities. When this information is used to try to manipulate us into taking political action that we might otherwise resist, or even abhor, far more serious threats to political privacy and the integrity of political identity occur. In this Part, I will (1) explore these threats and provide a taxonomy of them, (2) examine how they manifest themselves in the Cambridge Analytica scandal, (3) show how they threaten democracy and the rule of law, and (4) tie these phenomena to the issue of political privacy.

A. Threats to the Integrity of Individual and Collective Identity

Threats to the integrity of individual and collective identity come in many forms. In this sub-part, I will explore three such threats: what I call the movement to the extremes, the activation of identity to promote violence, and the manipulation of identity to sow political chaos. Each of these threats, which are threats to not just identity but also, as a result, self-determination, are described below.

1. Movement to the Extremes

An individual's activities in the digital world can be manipulated toward extremism, where one loses control of the self and turns toward illiberal, undemocratic values. Indeed, the "attention merchants" as Tim Wu calls them,[85] are designing algorithms that tend to steer users toward more extreme content, mostly because such content is often more likely to maintain engagement with the site, and more engagement typically means more revenue through advertisements embedded in the site.[86] Take YouTube as a prime example of this phenomenon. This social media site presently has two *billion* monthly active users who are uploading more than 500 hours of video *every minute*.[87] The *New York Times* described the site's algorithm, powered by artificial intelligence, as a "kind of long-term addiction machine . . . [that]

85. *See* TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS (2016).

86. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 457-59 (2019) (describing the Facebook algorithm that is designed to maintain engagement by end-users).

87. Kevin Roose, *The Making of a YouTube Radical*, N.Y. TIMES (June 8, 2019), https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html [https://perma.cc/NM4N-UZ95].

was designed to maximize users' engagement over time by predicting which recommendations would expand their tastes and get them to watch not just one more video but many more."[88]

Other social media sites, like Facebook, trigger basic human emotions that tend to drive people, both those who post and those who see posts, towards extremism. Social media algorithms tend to promote posts with the most engagements, spurring even greater engagement. What spurs such engagement is more provocative, extremist content, particularly that which triggers primal emotions like fear and anger.[89] What is more, as Max Fisher and Amy Taub of the *New York Times* argue, "Tribalism—a universal human tendency—also draws heavy engagement. Posts that affirm your group identity by attacking another group tend to perform well."[90] Even the subtle digital pyrotechnics that accompany engagement often spark dopamine, resulting in individuals craving more such rewards, leading to more engaging—read, extreme—content.[91] This has the effect of not only exposing people to more outrageous and tribal content, it also encourages people to produce more such content, meaning that they inhabit a persona—an identity—that is itself more extreme, angry, and tribal.[92] But not only does this phenomenon affect the psyche and identity, it often triggers violence, as the following discussion shows.

---

88. *Id.* The *Wall Street Journal* has described the YouTube algorithm as follows: "YouTube's recommendations often lead users to channels that feature conspiracy theories, partisan viewpoints and misleading videos, even when those users haven't shown interest in such content. When users show a political bias in what they choose to view, YouTube typically recommends videos that echo those biases, often with more-extreme viewpoints."

Jack Nicas, *How YouTube Drives People to the Internet's Darkest Corners*, WALL ST. J. (Feb. 7, 2018, 1:04 PM), https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478 [https://perma.cc/2PTQ-2JJA]. *See also* Max Fisher & Amanda Taub, *How YouTube Radicalized Brazil*, N.Y. TIMES (Aug. 11, 2019), https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html [https://perma.cc/3RBZ-AHBQ] (describing radicalizing influence of social media on politics in Brazil). For more critiques of the YouTube algorithm, see, for example, Zeynep Tufekci, *YouTube, the Great Radicalizer*, N.Y. TIMES (Mar. 10, 2018), https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html [https://perma.cc/E2BM-TBTM]; Paul Lewis, *'Fiction is Outperforming Reality': How YouTube's Algorithm Distorts Truth*, THE GUARDIAN (Feb. 2, 2018, 7:00 PM), https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth [https://perma.cc/S94F-BXAF]. For a critique that goes beyond the algorithm alone, see Becca Lewis, *All of YouTube, Not Just the Algorithm, is a Far-Right Propaganda Machine*, MEDIUM (Jan. 8, 2020), https://ffwd.medium.com/all-of-youtube-not-just-the-algorithm-is-a-far-right-propaganda-machine-29b07b12430 [https://perma.cc/C2BS-GJFX].

89. Max Fisher & Amanda Taub, *How Everyday Social Media Users Become Real-World Extremists*, N.Y. TIMES (April 25, 2018), https://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html[https://perma.cc/WU6C-HWTT].

90. *Id.*

91. Simon Parkin, *Has Dopamine Got Us Hooked on Tech?*, THE GUARDIAN (Mar. 4, 2018), https://www.theguardian.com/technology/2018/mar/04/has-dopamine-got-us-hooked-on-tech-facebook-apps-addiction [https://perma.cc/W7H9-VPJT](describing social media use and its relation to dopamine).

92. *Id.*

2. Activating Identity to Promote Violence

One of the most insidious ways in which social media platforms are being utilized to activate identity to undermine the rule of law is through mob-based violence and domestic terrorism, both in the United States and abroad. First, throughout the world, social media sites like Facebook and Twitter are being used by individuals to motivate mob violence that often has an ethnic, racial, or religious cast to it.[93]

Second, whether it is the Christchurch shooting in New Zealand or several acts of mass gun violence in the United States, the individuals responsible for these acts have often utilized social media to advance racist viewpoints and profess their alignment with white supremacist movements.[94] The Christchurch shooter even attempted to post a video of the shooting on social media in real time.[95] The video and the accompanying "manifesto" were both widely shared online through sites like 8chan. A spate of shootings tied to the site has led one of the founders of the site to call for it to be dismantled.[96]

Social media is clearly at the center of these violent acts and the proponents of such violence strive to harness identity-based biases, which they can propagate and advance on social media channels.[97] Such violence is often the manifestation of perceived threats to identity, as many of these white supremacist activists embrace the "replacement theory," which posits that demographic shifts throughout the world will result in a weakening of white prestige, economic well-

93. *See, e.g.*, Hannah Ellis-Petersen, *Facebook Admits Failings Over Incitement to Violence in Myanmar*, THE GUARDIAN (Nov. 6, 2018), https://www.theguardian.com/technology/2018/nov/06/facebook-admits-it-has-not-done-enough-to-quell-hate-in-myanmar [https://perma.cc/U24W-L9AY](describing Facebook's role in stoking violence directed toward racial and religious minorities in Myanmar).

94. *See, e.g.*, Lois Beckett & Sam Levin, *El Paso Shooting: 21-Year-Old Suspect 'Posted Anti-Immigrant Manifest'*, THE GUARDIAN (Aug. 4, 2019), https://www.theguardian.com/us-news/2019/aug/03/el-paso-shooting-21-year-old-suspect-in-custody-as-officials-investigate-possible-hate[https://perma.cc/35BE-8WFV] (describing social media use of mass shooter in El Paso, TX).

95. *See, e.g.*, Craig Timberg et al., *The New Zealand Shooting Shows How YouTube and Facebook Spread Hate and Violent Images – Yet Again*, WASH. POST (Mar. 15, 2019, 6:01 PM), https://www.washingtonpost.com/technology/2019/03/15/facebook-youtube-twitter-amplified-video-christchurch-mosque-shooting/ [https://perma.cc/6GK5-4ACY] (describing mass shooter in Christchurch, New Zealand and his use of social media).

96. Kevin Roose, *'Shut the Site Down,' Says the Creator of 8chan, a Megaphone for Gunmen*, N.Y. TIMES (Aug. 4, 2019), https://www.nytimes.com/2019/08/04/technology/8chan-shooting-manifesto.html [https://perma.cc/U55G-BW6F] (noting that the creator the 8chan site is calling for it to be shut down).

97. *See, e.g.*, Alexander Tsesis, *Terrorist Speech on Social Media*, 70 VAND. L. REV. 651, 656-59 (2017) (itemizing examples of online hate speech directed toward fomenting violence).

being, and authority.[98] Through their violent acts, with their deep connection to social media, the digital world, and identity, these individuals, those sympathetic to them, and those who may carry out such acts in the future threaten to undermine democracy and the rule of law.[99] A product of resistance to diversity and the fear that demographic shifts have already generated a weakening of their economic, cultural, and political positions as seen and appreciated through the lens of identity, these violent, lawless acts serve as a form of resistance to the self-realization and self-determination of others who do not share the identity of those carrying them out.[100] The digital world has become a place where such ideas and ideologies can spread; the real world is where they manifest in action.

3. Manipulating Identity to Sow Political Chaos

In addition to using information gleaned from social media to direct specific messages to specific people, interference in the 2016 election also included attempting to manipulate identity-based groups, even those that did not exist prior to such manipulation. In the most egregious example of this manipulation, it is alleged that Russian operatives organized a series of rallies designed to take place at the same location and at the same time. As a recent U.S. Senate Intelligence Committee report found, a Facebook page entitled "Heart of Texas," which was actually based in St. Petersburg, Russia, called for a rally to take place at noon on May 21, 2016, in front of the Islamic Da'wah Center in Houston.[101] The goal of the rally was purportedly to "Stop Islamization of Texas."[102] "Heart of Texas" eventually attracted over 250,000 followers.[103] At the same time—literally—another Russian-based Facebook group, entitled "United Muslims of America," organized another rally to occur at the same place, this was purportedly designed to "Save Islamic Knowledge" and organized by this fictional group attempting to impersonate an actual non-profit organization.[104]

98. Rosa Schwartzburg, *The 'White Replacement Theory' Motivates Alt-Right Killers the World Over*, THE GUARDIAN (Aug. 5, 2019), https://www.theguardian.com/commentisfree/2019/aug/05/great-replacement-theory-alt-right-killers-el-paso [https://perma.cc/7DHP-78VG].

99. *See generally* PAUL COLLIER, WARS, GUNS, AND VOTES: DEMOCRACY IN DANGEROUS PLACES (2009) (describing relationship between violence, democracy, and the rule of law).

100. For a historical example of an instance where violence undermined the rule of law, see DAVID LUBAN, LEGAL MODERNISM: LAW, MEANING AND VIOLENCE 346-48 (1997) (describing the breakdown of rule of law in pre-WWII Germany).

101. SELECT COMM. ON INTELLIGENCE, RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 2: RUSSIA'S USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS, S. Rep. No. 116-XX, at 47 (1st Sess. 2019) (Comm. Rep.).

102. *Id.* at 47.

103. *Id.*

104. *Id.*

This page, the Senate reported, had "connection to over 325,000 followers."[105] Individual accounts linked to both groups, probably Russian trolls, attempted to "exploit the country's most divisive fault lines."[106] Similar efforts targeted African Americans and individuals and groups associated with the Black Lives Matter movement, often promoting messages designed to discourage African Americans from voting for Hillary Clinton, mostly by discouraging them from voting altogether.[107]

In many ways, these examples help set the stage for the description of the specific example I will use to examine the ways in which different institutions may cooperate or clash in efforts to protect political privacy in private-law contexts: the events that constitute what has come to be known as the Cambridge Analytica scandal and its fallout to date. It is to those events that I now turn.

B. The Cambridge Analytica Scandal

Emotional appeals, driven by ties to identity, have been the stuff of politics and democracy since the birth of democracy in Greece over 2000 years ago.[108] In more modern times, mass media has led to political campaigns where such emotional and identity-based appeals are broadcast widely.[109] But at the same time, political operatives have long used marketing techniques to engage in micro-targeted advertising, first through direct mail, and now, through social media and other channels.[110] Today's political campaigns, particularly in the United States but also, increasingly, throughout the world, play out in social media, with such campaigns and the organizations that support them utilizing both search and marketing functions that attempt to create

105. *Id.*

106. *Id.*

107. *Id.* at 64.

108. *See generally* Alan Brinton, *Pathos and the "Appeal to Emotion": An Aristotelian Analysis*, 5 HIST. OF PHIL. Q. 207 (1988) (describing Aristotle's discussion of the use of rhetoric and emotional appeals).

109. *See, e.g.*, Rachel Withers, *George H.W. Bush's "Willie Horton" Ad Will Always Be the Reference Point for Dog-Whistle Racism*, VOX (Dec. 1, 2018, 4:10 PM), https://www.vox.com/2018/12/1/18121221/george-hw-bush-willie-horton-dog-whistle-politics [https://perma.cc/E73L-E2L9] (describing racially charged attack ad used by the 1988 campaign of George H.W. Bush against his opponent, Michael Dukakis).

110. On the role of direct mail and then social media in political communications, see JILL LEPORE, THESE TRUTHS: A HISTORY OF THE UNITED STATES 665-67 (2018) (describing role of direct mail in political communications); *Id.* at 729-38 (describing the emergence of the Internet and social media and their relationship to political communication).

psychological profiles of potential consumers based on their social media and digital activities.[111] The digital self these activities reflect becomes the target of political marketing efforts.[112] A close review of what has come to be known as the Cambridge Analytica scandal reveals how a private company, working in conjunction with a political campaign, utilized a range of information, including information about Facebook users, to serve to create profiles of such users as well as the individuals on those users' networks.[113] Those profiles were then used to determine the types of messages that would resonate with particular individuals to help influence their electoral choices.[114]

Cambridge Analytica was a UK-based company that closed down operations in mid-2018.[115] Prior to its dissolution, it engaged in a wide range of marketing activities. One area in which it focused, prior to its recent demise, was supporting political candidates and political causes, ranging from getting involved in elections for individual candidates to supporting such efforts as the "Leave" campaign in the Brexit vote in the United Kingdom in early 2016.[116] Its chief executive, Alexander Nix, described the company's use of personality profiling to understand consumer preferences.[117] It would do this by assessing individual's personality on the following dimensions: openness, conscientiousness, extraversion, agreeableness, and neuroticism.[118] A committee report of the United Kingdom's House of Commons explained that this approach would, for example:

> [Help] decide how to persuade American voters on the importance of protection of the second amendment, which guarantees the right to keep and bear arms. . . . [Nix explained] you might play on the fears of

111. Alex Hern, *Cambridge Analytica: How Did It Turn Clicks into Votes?*, THE GUARDIAN (May 6, 2018), https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie [https://perma.cc/2BFX-HYRC](describing Cambridge Analytica's use of personality profiling in political communication).

112. Jeff Chester & Kathryn C. Montgomery, *The Role of Digital Marketing in Political Campaigns*, 6 INTERNET POL'Y REV. 1, 4 (2017) (describing Facebook's "identity-based targeting paradigm" and its use in political campaigns).

113. Hern, *supra* note 111.

114. *Id.*

115. Nicholas Confessore & Matthew Rosenberg, *Cambridge Analytica to File for Bankruptcy After Misuse of Facebook Data*, N.Y. TIMES (May 2, 2018), https://www.nytimes.com/2018/05/02/us/politics/cambridge-analytica-shut-down.html [https://perma.cc/FL5F-VR8H].

116. Alex Hern, *Cambridge Analytica Did Work for Leave.EU, Emails Confirm*, THE GUARDIAN (July 30, 2019), https://www.theguardian.com/uk-news/2019/jul/30/cambridge-analytica-did-work-for-leave-eu-emails-confirm [https://perma.cc/RL7X-KUPS].

117. DIGITAL, CULTURE, MEDIA, AND SPORT COMMITTEE, DISINFORMATION AND 'FAKE NEWS': INTERIM REPORT, 2017-19, HC 5, AT 27 (UK).

118. *Id.* at 27-28.

> someone who could be frightened into believing that they needed the right to have a gun to protect their home from intruders.[119]

Cambridge Analytica became closely tied with a Russian-born American researcher, Aleksandr Kogan, who devised a polling application and then a so-called personality quiz—ubiquitous on social media—for Facebook through which he was able to obtain personal information about those who took the poll as well as the individuals on their social networks (through the permissions the poll respondents gave him in the terms of service of the application).[120] From the data Kogan obtained through tracking people's social media activities, including their history of "liking" posts on the site, an employee at Cambridge Analytica, in a co-authored article, would claim as follows: "Commercial companies, governmental institutions, or even one's Facebook friends could use software to infer personality (and other attributes, such as intelligence or sexual orientation) that an individual may not have intended to share."[121] This information was then used for targeted advertising.[122] As one former employee of Cambridge Analytica explained: "We exploited Facebook to harvest millions of people's profiles . . . and built models to exploit what we knew about them and target their inner demons."[123] Nix would brag about the company's support for President Trump's election bid in 2016: "We did all the research, all the data, all the analytics, all the targeting. We ran all the digital campaign . . . the television campaign and our data informed all the strategy."[124] While there is some debate over whether Cambridge Analytica used this sort of psychological profiling to support the election of Donald Trump in 2016,[125] it is clear that the Trump campaign both worked closely with Facebook in using ad targeting and relied on Cambridge Analytica for support in such efforts.[126]

---

119. *Id.* at 28.

120. Carole Cadwalladr & Emma Graham-Harrison, *How Cambridge Analytica Turned Facebook 'Likes' into a Lucrative Political Tool*, THE GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm [https://perma.cc/YE4P-QERZ].

121. Renaud Lambiotte & Michal Kosinski, *Tracking the Digital Footprints of Personality*, in 102 PROC. IEEE 1934, 1938 (2014).

122. Hern, *supra* note 111.

123. ZUBOFF, *supra* note 86, at 279.

124. Emma Graham-Harrison & Carole Cadwalladr, *Cambridge Analytica Execs Boast of Role in Getting Donald Trump Elected*, THE GUARDIAN (Mar. 21, 2018), https://www.theguardian.com/uk-news/2018/mar/20/cambridge-analytica-execs-boast-of-role-in-getting-trump-elected [https://perma.cc/UU8Z-7Z8B].

125. Nicole Karlis, *Julian Wheatland: I Want There to Be a More Balanced View of Cambridge Analytica*, SALON (July 27, 2019, 6:00 PM), https://www.salon.com/2019/07/27/julian-wheatland-i-want-there-to-be-a-more-balanced-view-of-cambridge-analytica/ [https://perma.cc/D2TM-JJSM].

126. YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 271-73 (2018) (describing Facebook's coordination with Cambridge Analytica and the Trump campaign in 2016).

This type of profiling is not new to politics, but it has changed in scope and power. As Yochai Benkler and his co-authors explain, the "dynamics that have increased the efficacy of big data analysis in general" include "Facebook's massive footprint; the increased storage and processing capacity to allow major platforms to refine and scale data analysis; and the development of machine learning algorithms to extract meaning from ever larger data sets."[127] Recently, the Federal Trade Commission (FTC) entered into a settlement with Facebook over the Cambridge Analytica scandal in which the company agreed to pay $5 billion for what the FTC said was a breach of a prior settlement with the agency over privacy violations by the site.[128] In Part IV, I will discuss litigation brought by private plaintiffs against Facebook for its actions in sharing personal data that was ultimately used by Cambridge Analytica.[129]

C. Activating Identity to Threaten Democracy

What these examples all have in common is that those who would utilize and activate aspects of identity to further their ends seem to appreciate the important role that identity plays in achieving such ends, whether they are strictly commercial, political, or nefarious. They seem to grasp what social change activists have understood probably since the beginning of civilization: individuals are motivated by feelings of solidarity and trust, which often emerge based on what network theorists call *propinquity*—that we tend to cluster based on perceived similarities.[130] We can identify with these similarities, but we can also be identified by them. In the social movement context, from the #MeToo Movement and Black Lives Matter to the constellation of groups labeled under the umbrella of the Alt-Right, there is more often than not an identity-based component to their organizing, whether one identifies as a victim and survivor of sexual harassment; police violence against communities of color; or perceived bias against conservatives, Christians and/or Caucasians.[131] In the digital sphere, the examples shown above reveal that entities and organizations that wish to pursue ad revenue, promote a political viewpoint, or stir electoral chaos or violence are also activating and manipulating notions of identity—whether it is to foster continued engagement with a site through

127. *Id.* at 272.

128. Cecilia Kang, *F.T.C. Approves Facebook Fine of About $5 Billion*, N.Y. TIMES (July 12, 2019), https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html [https://perma.cc/P2TH-LAXH] (describing FTC penalty imposed on Facebook for improperly sharing personal information of users with third parties).

129. *See infra* Part IV.

130. *See* CHARLES KADUSHIN, UNDERSTANDING SOCIAL NETWORKS: THEORIES, CONCEPTS, AND FINDINGS 18 (2012) (describing the concept of propinquity).

131. *See, e.g.*, FRANCIS FUKUYAMA, IDENTITY: THE DEMAND FOR DIGNITY AND THE POLITICS OF RESENTMENT 10-123 (2018) (describing different identity-based distinctions in American history).

algorithms that promote more extreme content based on the calculated interests of the individual to favor a particular political viewpoint, support a particular candidate, or foment violence. In each instance, identity is the fulcrum on which this activity hinges.[132] As such, it is appropriate to direct our attention to the ways in which identity is being used; the threats such phenomena pose to privacy, democracy, and the rule of law; and the laws currently in place and those that might emerge to protect the integrity of individual and collective identity.

The activation of identity-based interests and their manipulation in unwanted ways, both of which we see occurring in the examples provided above, undermine self-determination. An example of this occurred in the run-up to the 2016 presidential election. Research shows that individuals posing as affiliates of groups engaged with Black Lives Matter activism infiltrated such groups and spread information designed to discourage individuals within such networks from voting, or encouraged them to vote for third-party candidates.[133] The presumption was, based on the race and/or political inclinations of individuals within the network, that they were more inclined to vote for Hillary Clinton rather than Donald Trump.[134] If even some of these voters could be led to another candidate, or were convinced not to vote at all because they were told there was little difference between the candidates, that would result in fewer votes for Clinton.[135] Certainly, one can argue that these sorts of political marketing strategies are not new; such identity-based appeals are as old as democracy itself. But what is different is the combination of digital platforms and the knowledge that such platforms contain—and sell—about their users. In other words, at the center of much of these phenomena is the notion of privacy, or a lack thereof.

D. Connecting the Integrity of Political Identity to Privacy

As the previous discussion has shown, without privacy with respect to the core aspects of identity that individuals and groups may wish to

---

132. An example of how identity is playing out in electoral politics can be seen in the Trump campaign's challenges to the vote counts in particular areas which were notable for the high number of African-American voters found within them, such as Philadelphia, Milwaukee, and Atlanta. For a description of the Trump campaign's post-election challenges affecting such areas see Aaron Morrison et al., *Trump Election Challenges Sound Alarm Among Voters of Color*, AP NEWS (Nov. 22, 2020), https://apnews.com/article/joe-biden-donald-trump-race-and-ethnicity-georgia-wisconsin-a2f5155019a0c5aa09a7a6a82fb7d14b [https://perma.cc/K7D7-4GQP].

133. PHILIP N. HOWARD ET AL., COMPUTATIONAL PROPAGANDA RSCH. PROJECT, UNIV. OF OXFORD, THE IRA, SOCIAL MEDIA AND POLITICAL POLARIZATION IN THE UNITED STATES, 2012-2018 32-34 (2019), https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf#page=1 [https://perma.cc/QEN3-Z6FB] (describing social media efforts to "demobilize African Americans, LGBT, and liberal voters" from supporting Hillary Clinton in the 2016 election).

134. *Id.*

135. *Id.*

keep personal to themselves, such identity is subject to targeting, manipulation, and abuse. As Paul Schwartz argues: "Participation in a democracy requires individuals to have an underlying capacity for self-determination, which requires some personal privacy."[136] What the examples above show is that many have had and are having their individual identities exposed, used, and manipulated by private actors to achieve very political ends, and these ends are not necessarily those that the subjects of that exposure would choose. What is more, knowledge of the fact that much of this critical personal information is subject to use and abuse by third parties is likely to have a chilling effect, preventing individuals from engaging in behavior they would otherwise prefer to remain private, especially activities by and on behalf of marginalized groups.[137] When individuals are hesitant to or refuse to engage in coordinated associational activity for fear that such activities might reveal their identities and their affinities might be exposed, manipulated, and abused, the real and lasting benefits of such activity will not materialize. This, in turn, undermines individual and collective self-determination.

What these phenomena all reveal is that information about many who utilize digital technologies is readily available to those who would access it for their own ends, and such information is being manipulated to not just hack identity but also democracy itself. In turn, these acts have profound effects on the integrity of individual and collective identity and the advancement of social change. The next Part explores the ways in which existing protections for political privacy in the market and through the political process may or may not preserve the integrity of individual and collective identity.

III. COMPARING THE RELATIVE STRENGTHS OF THE INSTITUTIONS THAT MIGHT PROTECT DIGITAL PRIVACY ON THEIR OWN

In order to determine the best method or methods through which to protect the integrity of identity through private-law means, we can assess the different institutional contexts in which we might effectuate this protection. As the following discussion shows, a means by which to conduct this type of assessment is through the process known as comparative institutional analysis.

136. Paul M. Schwartz, *Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes's Jorde Lecture*, 97 CALIF. L. REV. 407, 408 (2009).

137. *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 488 (2006) (describing "chilling effect" of government surveillance which might make individuals "less likely to attend political rallies or criticize popular views"). *Unlawful Surveillance Threatens Our Activism. Here's How We Can Fight Back*, AMNESTY INTERNATIONAL (Nov. 8, 2015) https://www.amnestyusa.org/unlawful-surveillance-threatens-our-activism-heres-how-we-can-fight-back/ [https://perma.cc/79FE-PKLW] (last visited July 23, 2021) (describing threats to activism due to surveillance).

A. Comparative Institutional Analysis

Comparative institutional analysis arose in the early 1990s as a way to think about the pursuit of policy goals, that is, as a process embedded within an institutional framework.[138] While the term institutions can take on many meanings, the scholar most associated with the comparative institutional approach, Neil Komesar,[139] spoke of institutions broadly and categorized them into three types: the government, the market, and the courts.[140] For Komesar, in order to achieve desired policy goals, one must analyze not just each such institution as a field in which policy decisions and the policy-making function may reside, but rather one must also compare these different institutional systems (as I prefer to call them) against each other in a particular policy-making realm.[141] That is, in a particular policy arena, the courts may be in a better position to achieve the desired policy goal than that of the political system or the market.[142] This comparative approach is better, from Komesar's perspective, than what he calls "single institutionalism," that is, when one weighs whether a single institutional system is appropriate to achieve one's goals, without assessing whether it is superior to another.[143] Such an approach, he argues, fails to appreciate the value of comparing the functioning of multiple institutions in particular contexts to determine the institution best suited to meet the intended goals.[144] While one can certainly analyze the strengths and weaknesses of a particular institutional setting in achieving a particular policy goal or goals, such an institutional system may have such strengths and weaknesses, but one will not know whether, in light of those strengths and weaknesses, one system is superior to another: whether, on the whole, the strengths of one system outweigh those of another, while the weaknesses pose less of a barrier to achieving the desired policy goals. In other words, one can criticize a particular institutional system, but despite those criticisms and any weaknesses a system may exhibit, it might still stand a greater chance of achieving the desired goals than another institutional system.

Generally speaking, when analyzing institutions, it is useful to determine whether they possess particular characteristics that might make them better suited to achieve a particular policy outcome. For example, Komesar identifies three distinct characteristics of courts

138. KOMESAR, IMPERFECT ALTERNATIVES, *supra* note 23, at 4-5. For an intellectual history of the emergency of comparative institutional analysis alongside several other schools of thought, including Law & Economics and Critical Legal Studies, see generally Edward L. Rubin, *Institutional Analysis and the New Legal Process*, 1995 WIS. L. REV. 463 (1995) (reviewing KOMESAR, IMPERFECT ALTERNATIVES (1994)).

139. *See* KOMESAR, IMPERFECT ALTERNATIVES, *supra* note 23, at 4-5.

140. *Id.* at 9.

141. *Id.* at 5-8.

142. *Id.* at 5.

143. *Id.* at 6.

144. *Id.* at 4-7.

when compared to the market and the political process: "higher threshold access costs, limited scale, and judicial independence."[145] What is more, although one can identify such characteristics and determine whether they might pose barriers to effective use of the courts as an arena through which desired policy objectives might be achieved, one still has to weigh these characteristics against similar characteristics of other institutions to identity the comparative superiority of one system over another.[146] Furthermore, Komesar argues that the components of the judiciary's limited access are a product of concerns about preserving the proper role of the courts based on our collective understanding of what that institutional role should be in the distinctively American system.[147]

Komesar famously analyzed the New York Court of Appeals' decision in *Boomer v. Atlantic Cement Co.*[148] to highlight a situation in which the courts were in a position to exercise their authority to achieve particular policy goals in a manner that was superior to the capacity of other institutions to achieve similar outcomes.[149] There, residents of upstate New York sought an injunction to halt noxious emissions from a cement plant.[150] The court ultimately concluded that to achieve the policy goal of economic efficiency, the economic value of the plant's activities was superior to the economic loss of the residents; as a result, the appropriate remedy to achieve the desired goal of greater efficiency was simply to order the defendant to compensate the plaintiffs for their harm from the plant's emissions.[151] For Komesar, the court in *Boomer* was in the best position relative to the political process or the market to achieve the goal of resource allocation efficiency.[152] Market transactions would have involved untenable negotiations with a large number of people and a single holdout might undermine an efficient outcome.[153] Similarly, the political process might have resulted in an unfair and inefficient allocation of resources if one party might capture or otherwise dominate the levers of political power.[154] Komesar concludes that in this setting, to achieve the desired policy goal, one can see that the courts were in the best position—relative to other institutional settings—to accomplish that goal.[155]

145. *Id.* at 123.

146. *Id.* at 123.

147. *See id.* at 123-50.

148. 26 N.Y.2d 219 (1970).

149. *See* KOMESAR, IMPERFECT ALTERNATIVES, *supra* note 23, at 14–28.

150. *Boomer*, 26 N.Y.2d at 222.

151. KOMESAR, IMPERFECT ALTERNATIVES, *supra* note 23, at 16.

152. *See id.*

153. *Id.* at 19.

154. *Id.* at 26-27. This tension also exposes what Komesar calls the potential majoritarian and minority biases present, at times, in different institutional systems. *See id.* at 56-81.

155. *See id.* at 21, 26-27.

Policy goals, the scale of problems, and the number of people involved in a particular policy setting may change over time, which have ramifications for the functioning of different institutions in different situations. Indeed, the scope and scale of environmental degradation have both increased over time, as has the complexity of the problem. For Komesar, the capacity of institutions to function effectively can deteriorate as problems grow and become more complex.[156] When the number of people involved in market transactions and disputes that emerge from them grow, their complexity grows, and the ability of institutions to achieve desired policy goals weakens.[157] Indeed, transactions costs rise, negotiations become more complicated,[158] political processes can become gridlocked by diverse needs of competing constituencies,[159] and contested litigation can become more complicated with more parties and more issues to resolve.[160] Political processes can become paralyzed when they attempt to meet the conflicting needs of a diverse electorate, which can lead to their capture by a powerful elite. Thus, the effectiveness of the Komesarian institutions at the heart of traditional comparative institutional analysis weakens when the number of individuals involved in a particular setting increases and the complexity of their problems grow.[161] While institutions may have a harder time responding effectively to policy challenges and bringing about desired policy goals when the scope, scale, and complexity of a particular setting grow, that does not mean we should discard the comparative institutional approach to identifying the appropriate institution for achieving desired policy outcomes.[162] Rather, it just means that such analysis is, itself, more difficult and complex.[163]

In my own research, I have argued that there is another way to utilize comparative institutional analysis, particularly in settings where the size, scope, and complexity of the problem are all high. Indeed, I have argued that we could advance the field of comparative institutional analysis by viewing institutions in a somewhat more nuanced fashion.[164] In this view, what I have called a "multi-dimensional" approach to comparative institutional analysis, one takes into account the fact that institutions are not themselves monolithic, but rather

156. NEIL K. KOMESAR, LAW'S LIMITS: THE RULE OF LAW AND THE SUPPLY OF DEMAND AND RIGHTS 159-60 (2001) [hereinafter KOMESAR, LAW'S LIMITS].

157. *Id.* at 160.

158. *See* Neil Komesar, *The Logic of the Law and the Essence of Economics: Reflections on Forty Years in the Wilderness*, 2013 WIS. L. REV. 265, 299-301 (2013) [hereinafter Komesar, *The Logic of the Law*].

159. *See* KOMESAR, LAW'S LIMITS, *supra* note 156, at 116-22.

160. *See generally* KOMESAR, IMPERFECT ALTERNATIVES, *supra* note 23, at 177-95.

161. Komesar, *The Logic of the Law*, *supra* note 158, at 300.

162. *Id.*

163. *Id.*

164. *See generally* Raymond H. Brescia, *Understanding Institutions: A Multi-Dimensional Approach*, 17 U.N.H. L. REV. 1 (2018).

have a range of aspects to them such that we cannot and should not compare them individually against each other. I have shown, using the environmental dispute at the center of the Supreme Court's decision in *Massachusetts v. Environmental Protection Agency*,[165] that institutions have multiple dimensions and we should engage in comparative institutional analysis with an appreciation for the ways in which institutions operate—a form of micro-analysis of institutions, institutional roles, and institutional norms and behaviors.[166]

In this view of institutions, at least in the American system, such institutions reflect a great deal of heterogeneity and they do so across a range of what I call "dimensions."[167] Institutions reflect vertical heterogeneity in that each of the Komesarian institutions will have different structural components that create levels within the institution: for example, local, state, and federal governments; trial courts and appellate courts.[168] Sometimes the entities and leaders found at these different levels can work collaboratively, sometimes uncooperatively, meaning it is not always possible to assess how one particular institutional setting—for example, the political process—approaches a policy problem because these different levels may approach it differently.[169] Institutions also reflect horizontal heterogeneity: a government or court system may have different components like a legislature and executive branch; the private sector has businesses and non-profit entities embedded within it.[170] Entities within different institutions will also have different roles, like a legislature that makes the law and an administrative agency that provides regulatory oversight.[171] They will also have different interests, even when they may occupy the very same role; for example, the state attorney general from one state may sue the federal government to prevent a policy from going into effect, and another state attorney general may sue to ensure that it does.[172]

165. 549 U.S. 497, 560 (2007).

166. Borrowing from Heather Gerken, I have referred to this approach to institutional analysis as institutional analysis "all the way down." Brescia, *supra* note 164, at 5; *see* Heather K. Gerken, *Federalism All the Way Down*, 124 HARV. L. REV. 4, 9-10 (2010) (calling for a view of federalism that looks at institutions at the hyper-local level, what she calls "Federalism all the way down").

167. *See* Brescia, *supra* note 164, at 39-56.

168. *See id.* at 39-41.

169. These disputes can be amplified when the different levels of government are occupied by different political parties, a process one author calls "[p]artisan federalism." Jessica Bulman-Pozen, *Partisan Federalism*, 127 HARV. L. REV. 1077, 1080 (2014).

170. Brescia, *supra* note 164, at 41-42.

171. *Id.* at 42-45.

172. *See, e.g.*, Alana Abramson, *White House Says President Trump 'Wrestled' with Decision to End DACA*, TIME (Sept. 5, 2017, 3:16 PM), https://time.com/4927934/daca-dreamers-trump-wrestled/ (describing pressure the Trump Administration faced from litigation commenced by conservative state attorneys general over DACA program); Tal Kopan, *Blue States Sue Trump Over DACA*, CNN (Sept. 6, 2017, 7:07 PM), http://www.cnn.com/2017/09/06/politics/daca-trump-states-lawsuits/index.html (describing lawsuits by progressive states against the Trump Administration over immigration policies).

The heterogeneity of different institutions thus means they may operate at cross-purposes, resisting efforts to achieve certain goals, mostly because these different institutional actors may have different policy goals and may pursue them in the face of opposition from other actors within the same institutional setting or those from other settings.

Critical to our conversation, though, it is important to recognize that institutions can also be interdependent, pursuing particular policy goals together, like where a private entity, like the American Bar Association (ABA), partners with government to provide oversight over law schools or generates model rules regarding the ethical responsibility of lawyers within the legal profession.[173] Similarly, the line between institutions can become blurred, as when a private arbitrator undertakes a dispute resolution function and that function is overseen by the courts.[174] Finally, I have argued that institutions reflect a temporal heterogeneity, particularly in their interests—elections can change the focus of a legislative body or executive position virtually overnight.[175]

Using this multi-dimensional lens for viewing institutions, I will assess the most effective methods or methods for providing protections for political privacy, recognizing that, in the end, the different institutional settings in which such privacy can be protected, and even enhanced, likely need to work together to achieve this desired goal—assuming that is the goal that most consumers want and desire. While I will use this multi-dimensional approach to assess the appropriate institutional setting or settings for protecting political privacy, for ease of analysis, I will start from the Komesarian view of institutions and attempt to assess the relative effectiveness of two of them—the markets and the political process—in providing robust consumer protections for political privacy. In this Part, I will assess whether these two institutions, standing alone, would be the comparatively superior institution to serve as the locus for digital privacy. As this discussion reveals, these two institutional settings, working independently and individually, have proven ineffective in securing political privacy. What is more, they have effectively impacted the ability of the third of Komesar's institutions—the courts—to serve as a strong check on violations of political privacy by private actors.

---

173. For a critical description of the ABA's law school accreditation process, see generally Matthew D. Staver & Anita L. Staver, *Lifting the Veil: An Exposé on the American Bar Association's Arbitrary and Capricious Accreditation Process*, 49 WAYNE L. REV. 1 (2003). For a description of the process by which the ABA adopted the Model Rules of Professional Conduct, see CHARLES W. WOLFRAM, MODERN LEGAL ETHICS 60-63 (1986).

174. *See* Judith Resnik, Comment, *Fairness in Numbers: A Comment on AT&T v. Concepcion, Wal-Mart v. Dukes, and Turner v. Rogers*, 125 HARV. L. REV. 78, 112-18 (2011) (describing expansion of adjudication through private arbitration of civil disputes in the United States).

175. Brescia, *supra* note 164, at 52-56.

B. *Institutions and Privacy*

In this next section, I will discuss the ways in which two of Komesar's institutions—the market and the political process—have or have not, to date, provided sufficient protection for political privacy. As the following discussion shows, both the private sector and the political process have created a legal infrastructure that has, for the most part, shielded many entities that hold private information from accountability, enabling them to sell and share such information largely immune from oversight. As a result, it is easy to see that these two institutional systems are not currently serving in an effective way to protect digital privacy, and, by extension, political privacy.

When we look at the institutions of the private and public sectors, four types of immunities have emerged that have mostly insulated holders of digital information from accountability for their uses and abuses of personal information. I have called these contractual immunity, adjudicative immunity, statutory immunity, and enforcement immunity.[176] In many ways, the actions and inactions of these sectors in cooperating to an extent in realizing these immunities make them all the more powerful and protective of the private sector. The fact that these immunities are a product of this interchange between sectors likely means solutions to addressing digital privacy will also require a cross-institutional response. What follows is a discussion of the ways in which these immunities play out from within and between the institutions of the market and the public sector, showing that these institutions are not, at present, serving to protect political privacy.

1. *Private Sector*

The first of the immunities outlined is contractual immunity.[177] When private companies operate in the digital world, they have access to a range of their customers' digital information.[178] Contractual agreements governing the use of such data authorize companies to use their customers' data,[179] and such contracts tend to be opaque and one-sided

176. *See* Brescia, *Zoning Cyberspace*, *supra* note 74, at 28-29.

177. For an overview of the scholarship on contractual immunity, see, for example, Margaret Jane Radin, *Boilerplate Today: The Rise of Modularity and the Waning of Consent*, *in* BOILERPLATE: THE FOUNDATION OF MARKET CONTRACTS 189, 189-192 (Omri Ben-Shahar ed., 2007) [hereinafter, BEN-SHAHAR, FOUNDATION OF MARKET CONTRACTS].

178. BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 209-10 (2018) (describing tendency of consumer to accept the terms contained in terms-of-service agreements).

179. NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS 48-49 (2013) (describing contracts as both a sword and a shield, protecting providers but also stripping counter-party of rights).

with an asymmetry of information regarding the terms of the agreements protecting providers.[180] While the adoption of new rules for the European Union and the state of California may make it more difficult for providers to enter into such one-sided contracts, such asymmetries will likely remain to a great extent or providers will find ways to satisfy the requirements of these and other protections while preserving their contractual immunity.[181]

The second type of immunity, which, in many ways, is a close cousin to contractual immunity because this immunity is often embedded within the contracts that create the contractual immunity, is what can be referred to as adjudicative immunity. The terms of service of many digital providers include provisions that require that any dispute under the agreement is to be resolved through arbitration,[182] and such arbitration agreements often bar class arbitration.[183] Such provisions are generally highly favorable towards those they insulate from judicial review, partially because consumers are less likely to pursue such arbitrations, especially when to do so is more expensive to prosecute than if those consumers banded together to bring their actions as a class.[184]

---

180. MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 7-16 (2013) [hereinafter RADIN, BOILERPLATE] (describing the asymmetries of information between consumers and companies). Even where companies have claimed to preserve their customers' data through techniques such as anonymization, data breaches, which reveal personal information, are common. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1717-22 (2010) (describing the failure of anonymization technologies to preserve privacy in several data breach incidents).

181. For an analysis of tort liability under the European Union's new privacy standards and the state of California's new privacy rules, see generally Rustad & Koenig, *supra* note 12, at 365. For a discussion of how financial institutions were able to satisfy disclosure requirements in financial reform legislation without undermining the protections they enjoyed from liability, see CASS R. SUNSTEIN, HOW CHANGE HAPPENS 102-04 (2019).

182. *See, e.g.*, Jeremy B. Merrill, *One-Third of Top Websites Restrict Customers' Right to Sue*, N.Y. TIMES (Oct. 23, 2014), https://www.nytimes.com/2014/10/23/upshot/one-third-of-top-websites-restrict-customers-right-to-sue.html [https://perma.cc/GZ82-V5J7] (describing the prevalence of arbitration agreements in online terms-of-service agreements); *see also* RADIN, BOILERPLATE, *supra* note 180, at 133-134 (describing reasons providers insert arbitration clauses in terms-of-service agreements and other contracts).

183. *See* Am. Express v. Italian Colors Rest., 570 U.S. 228, 238 (2013) (holding waiver of class arbitration enforceable even where individual arbitration of dispute is impracticable).

184. *See generally*, David Horton & Andrea Cann Chandrasekher, *After the Revolution: An Empirical Study of Consumer Arbitration*, 104 GEO. L. J. 57, 57 (2015); *see, e.g.*, AT&T Mobility v. Concepcion, 563 U.S. 333, 348 (2011) (upholding class-wide arbitration waiver); Resnik, *supra* note 174, at 122 (raising questions about equality and fairness in enforcement of arbitration clauses); Ann C. Hodges, *Can Compulsory Arbitration Be Reconciled with Section 7 Rights*, 38 WAKE FOREST L. REV. 173, 218-19 (2003) (describing chilling effect arbitration clauses have on concerted litigation activity by plaintiffs). *But cf.* Jason Scott Johnston, *Cooperative Negotiations in the Shadow of Boilerplate*, *in* BOILERPLATE: THE FOUNDATION OF MARKET CONTRACTS 27-28 (Omri Ben-Shahar ed., 2007) (arguing that arbitration clauses in consumer contracts bring benefits to consumers); *see also*, David Dayen, *Tech Companies' Big Reveal: Hardly Anyone Files Arbitration Claims*, AM. PROSPECT (Nov. 26, 2019),

There are two ways in which the market, standing alone, could strengthen digital privacy. The first is for companies to continue to self-regulate, to strive, through their own internal practices, to improve and enhance the protections they afford their customers. This is certainly the preferred regulatory approach of the private sector.[185] The argument is that these entities are in the best position to understand their product and have their customers' interests in mind.[186] They also argue that onerous regulation and oversight from outside forces would stifle innovation and limit the ability of the private sector to continue to provide innovative, useful, attractive, and effective products.[187] While there is some value to permitting companies that provide digital services to have some degree of leeway in the products they design and market, there is currently little support for the notion that they are in a position to police themselves effectively.[188] The truth is, they seem to be doing a terrible job of doing so at present. There is a robust effort underway to raise awareness of the current state of digital privacy, which is leading many to clamor for stronger protections.

Still, there are those who believe extensive regulation of digital privacy is unnecessary moving forward, even if private industry has not established strong guardrails to date.[189] A continuing argument for allowing the market to police itself is that the market will, in the end, serve as the best disciplining force for internet companies: consumers will vote with their feet and their wallets and take their business elsewhere if they do not like the practices of such companies, creating a

---

https://prospect.org/power/tech-companies-hardly-anyone-files-arbitration-claims/ [https://perma.cc/V5Q4-Z874] (noting the "trivial number" of arbitration claims filed against nation's largest technology companies).

185. Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (U.S. Dep't of Commerce ed., 1997), https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy [https://perma.cc/A75K-AVXD] (noting industry typically prefers self-regulation of privacy issues).

186. *See, e.g.*, David C. Grossman, *Blaming the Victim: How FTC Data Security Enforcement Actions Make Companies and Consumers More Vulnerable to Hackers*, 23 GEO. MASON L. REV. 1283, 1312-17 (2016) (arguing for an approach to enforcement of data breaches that will not chill action and stifle innovation).

187. W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 405, 418-19 (2019) (describing self-regulatory approach favored under U.S. privacy laws as they affect private entities). As Anupam Chander points out, this was the position embraced by the Clinton Administration in the 1990s. *See* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L. J. 639, 648-49 (2014) (describing the Clinton Administration's preference for self-regulation for internet companies).

188. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1286-87 (noting "abject failure" of self-regulation to protect information privacy).

189. Indeed, some see passage of a federal privacy law as a means of preempting more onerous state privacy laws. *See* Electronic Frontier Foundation, Letter to Chairman John Thune & Ranking Member Bill Nelson, U.S. Senate Committee on Commerce, Science & Transportation (Sept. 24, 2018), https://www.eff.org/files/2018/09/24/eff_letter_to_senate_commerce_on_consumer_privacy_sep_24_2018-_preemption_concerns.pdf [https://perma.cc/ENJ9-PEER] (describing industry preference for federal privacy law to preempt state laws).

race-to-the-top in which companies compete to have the best products and services that offer consumers the highest and most effective digital privacy.[190]

But there are several arguments that undermine this thinking. The first is that some of the companies that are the most aggressive about harvesting and selling their customers' personal data have established too large a presence in the market such that they are able to crowd out competitors.[191] They have established considerable network endowments and generate network effects that significantly diminish the attractiveness of alternate providers. Indeed, in the social media space, the network is the providers' critical strength.[192] The relative cost of not just switching platforms to a more protective service but also getting everyone in one's network to switch platforms is high.[193] Thus, the effectiveness of a market-only approach to digital privacy is minimal. While there is always some degree of validity to the argument that entrepreneurs and those who would innovate in any sector need legal and regulatory space to do so, there is also the risk that such leeway will continue to create a sort of moral hazard, where weak regulations lead to predatory conduct and rent-seeking.[194] Moreover, as Dennis Hirsch has argued, such abusive privacy practices can lead consumers to distrust providers to such an extent that they abandon the market altogether.[195] Legal and regulatory oversight can lead to the trust that is necessary to maintain customer engagement and sustain economic activity, especially in situations where mistrust is high.[196] Thus, given

190. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 550 (2009) (describing market-based view that self-regulation will encourage competition and better industry practices around privacy).

191. This concentration poses significant risks to political privacy. As Frank Pasquale has argued, when discussing the need for the concept of net neutrality, "[c]orporate forces menace both user privacy and free expression on the Internet. Market concentration lets powerful business leaders develop unprecedented digital dossiers on users. Such concentration also allows leading companies to pervasively shape culture and politics, elevating some voices and silencing others." Frank Pasquale, *Search, Speech, and Secrecy: Corporate Strategies for Inverting Net Neutrality Debates*, YALE L. & POL'Y REV. INTER ALIA (May 15, 2010, 10:15 AM), https://ylpr.yale.edu/inter_alia/search-speech-and-secrecy-corporate-strategies-inverting-net-neutrality-debates [https://perma.cc/Z7WV-B93U].

192. On the network effects enjoyed by "tech giants," including Facebook, see Eleanor M. Fox, *Platforms, Power, and the Antitrust Challenge: A Modest Proposal to Narrow the U.S.-Europe Divide*, 98 NEB. L. REV. 297, 304-05 (2019).

193. For a discussion of network effects and switching costs, see Ruben Rodrigues, *Privacy on Social Networks: Norms, Markets, and Natural Monopoly*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 237, 244-45 (Saul Levmore & Martha C. Nussbaum eds., 2010).

194. *See* Jeffrey L. Vagle, *Cybersecurity and Moral Hazard*, 23 STAN. TECH. L. REV. 71, 72-82 (2020) (describing the role of moral hazard in the protection of data privacy).

195. Dennis D. Hirsch, Response, *Privacy, Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel*, 65 DUKE L. J. ONLINE 67, 70 (2016).

196. For a discussion of the role of law in fostering trust, see generally Carol M. Rose, *Trust in the Mirror of Betrayal*, 75 B.U. L. REV. 531, 531-33 (1995).

the fact that the public, legislators, and regulators have begun to question the effectiveness of self-regulation to govern political privacy, are there other institutional settings where protection for such privacy should reside?

2. *Political Process/Government Sector*

If the market cannot police itself, could the political process serve as an effective setting through which we can regulate digital privacy? There is something to the argument that the public sector does not quite understand the industry and may not be in the best position to regulate it if left to its own devices, so to speak. Famously, one legislator displayed an utter lack of understanding of the social media business model when, in a congressional hearing, he asked Facebook CEO Mark Zuckerberg to explain how the company generated revenue if it did not charge its customers, leaving Zuckerberg to explain that advertising *to* its user base was Facebook's source of income.[197]

Another fear regarding public sector oversight is that it is susceptible to capture, whether administrative or legislative.[198] Such capture can lead to the adoption of rules that weaken, rather than advance, digital privacy, especially in the event the U.S. Congress passes legislation that preempts state-based efforts to protect digital privacy, as some fear will happen if a federal digital privacy bill advances and becomes law.[199] And if digital privacy is not protected, political privacy is also exposed. While there is certainly room for legislatures to pass legislation; law enforcement authorities to investigate and prosecute privacy violations (which would involve engagement with another institution—the courts); and administrative agencies to provide some oversight using existing laws and regulations, the political setting, standing alone, likely would prove an ineffective institutional setting to secure digital and, by extension, political privacy. Take, for example, the third type of immunity listed above—statutory immunity—as an example of one way in which the political process has helped to insulate many digital providers from accountability for the information shared on their platforms. The most powerful piece of legislation in providing

197. Emily Stewart, *Lawmakers Seem Confused About What Facebook Does—And How to Fix It*, VOX (Apr. 10, 2018, 7:50 PM), https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations [https://perma.cc/4G5Y-ZA29].

198. Lital Helman, *Pay for (Privacy) Performance: Holding Social Network Executives Accountable for Breaches in Data Privacy Protection*, 84 BROOK. L. REV. 523, 554 (2019) (discussing risks of capture in privacy oversight). On capture generally, see Roger G. Noll, *The Behavior of Regulatory Agencies*, 29 REV. SOC. ECON. 15 (1971). On the ways in which capture theory can influence and aid comparative institutional analysis, see Thomas W. Merrill, *Capture Theory and the Courts: 1967-1983*, 72 CHI.-KENT L. REV. 1039, 1051-52 (1997).

199. Bennett Cyphers et al., *Tech Lobbyists Are Pushing Bad Privacy Bills. Washington Can, and Must, Do Better.*, ELECTRONIC FRONTIER FOUND. (Mar. 6, 2020), https://www.eff.org/deeplinks/2020/03/tech-lobbyists-are-pushing-bad-privacy-bills-washington-state-can-and-must-do[https://perma.cc/6CC4-BSPQ].

this immunity is the Communications Decency Act (CDA),[200] which immunizes internet platforms from liability for the content supplied by third parties on their sites.[201] This can insulate such platforms from liability for privacy breaches, discriminatory content, and libel.[202]

Finally, another immunity that emerges through the political system is that law enforcement entities have proven less aggressive in policing digital privacy than we might hope. While the Federal Trade Commission (FTC) has taken some steps to police data privacy, it has failed to take aggressive action despite privacy breaches.[203] For example, although Facebook settled claims with the FTC over the company's involvement in the Cambridge Analytica scandal,[204] some commentators argue that the fine would do little to deter Facebook from similar conduct in the future.[205] The failure of the FTC to take significant action with other data breaches leaves many concerned that the entity does not have the capacity or desire to police data privacy.[206] State attorneys general have taken some steps to protect digital privacy, but they do not have the resources that the federal government has to police privacy practices.[207]

---

200. 47 U.S.C. § 230(c)(1).

201. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (holding that "[b]y its plain language, §230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service").

202. On the emergence and importance of the CDA, see generally JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019). On the purposes behind the CDA, see Chander, *supra* note 187, at 651-52.

203. *But see* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015) (upholding FTC authority to prosecute companies for data breaches).

204. *See* Hern, *supra* note 111 (describing Cambridge Analytica's use of personality profiling in political communication).

205. *See, e.g.*, Swisher, *supra* note 15 (criticizing the amount of the Facebook FTC fine as ineffective in discouraging future misbehavior).

206. *See* Josephine Wolff, *Filling the Cybersecurity Void*, SLATE (Apr. 17, 2019, 12:56 PM), https://slate.com/technology/2019/04/equifax-data-breach-aftermath-canada-united-states.html [https://perma.cc/GH92-Y9NN] (criticizing FTC for lack of aggressive enforcement in data breach incidents).

207. Still, some state attorneys general have taken steps to rein in poor privacy practices. *See, e.g.*, Press Release, Att'y Gen. of the State of N.Y., AG James Sues Dunkin' Donuts for Glazing Over Cyberattacks Targeting Thousands (Sep. 26, 2019), https://ag.ny.gov/press-release/2019/ag-james-sues-dunkin-donuts-glazing-over-cyberattacks-targeting-thousands [https://perma.cc/S66F-RNZ8]; *see also* Robert R. Kuehn, *The Limits of Devolving Enforcement of Federal Environmental Laws*, 70 TUL. L. REV. 2373, 2388-95 (1996) (arguing, in the environmental context, that federal enforcement is generally stronger than state enforcement). *But see* Michele M. Bradley, *The States' Role in Regulating Food Labeling and Advertising: The Effect of the Nutrition Labeling and Education Act of 1990*, 49 FOOD & DRUG L.J. 649, 672-74 (1994) (arguing states can play a complementary law enforcement role to federal authorities); Margaret H. Lemos, *State Enforcement of Federal Law*, 86 N.Y.U. L. REV. 698, 751-52 (2011) (arguing greater experimentation can emerge from federal and state law enforcement efforts).

3. *Private and Public, Working Together*

The four immunities, particularly when combined together, make it exceedingly difficult to police and protect digital privacy, which, in turn, makes it hard to preserve political privacy. In one way, the risks to political privacy threaten democracy itself, creating, as Radin argues, a "democratic degradation" of democracy because they undermine democratic self-determination and the will of the people to preserve their interests.[208] What is more, by relegating many decisions around the preservation of political privacy into individual acts between consumers and the companies that maintain their personal private information, "enforcement mechanisms that rely upon individual initiative often fail because individuals lack the knowledge and resources to use them."[209] And when the weaknesses in privacy institutions are structural, and not individual, "individual remedies are often powerless."[210]

Anupam Chander has described the way in which, as he says, law "made Silicon Valley,"[211] not through onerous, command-and-control oversight, but, rather, by having all sectors of government take a hands-off approach to regulation of the internet generally:

> [E]ach of the branches of government play[] an integral part in this endeavor. In the face of calls for legal protections, the Clinton Administration promoted self-regulation by the Internet industry. Congress wrote a set of statutes that dealt with some of the principal concerns of both the content industry and the public, without placing too much in the way of burdensome constraints on Silicon Valley enterprise.[212]

But Chander also points out that the courts "sought to protect speech and promote innovation by reading immunity statutes broadly and striking down statutes that might chill speech."[213] What is more, "each of the branches checked the others when they proved less than friendly to Internet innovation," and this "ultimately add[ed] up to a powerful set of pro-Internet laws."[214]

What this shows is that the different institutional settings—the market, the political process, and the courts—have largely worked together to create an environment where digital privacy is largely unprotected. Yet, in a series of cases, particularly one involving the Cambridge Analytica scandal, courts are demonstrating an ability to step in to adjudicate disputes over digital privacy and the plaintiffs are

208. RADIN, BOILERPLATE, *supra* note 180, at 16.

209. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 97 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON].

210. *Id.*

211. *See* Chander, *supra* note 187, at 647.

212. *Id.* at 649.

213. *Id.*

214. *Id.* at 649-50.

finding an ability to rein in some of the worst violations of that privacy.[215] They are largely doing so through an avenue that is somewhat insulated from meddling from the market or political institutions—the common law in the form of tort protections. The next Part explores the ways that courts may exhibit an institutional superiority, relative to the market and political processes, to protect digital privacy, and, by extension, political privacy.

IV. THE COURTS AND DIGITAL, POLITICAL PRIVACY

While the market and the political process have proven incapable, at least up to the present, of providing adequate protection for political privacy, can the courts, relatively speaking, prove superior to these other sectors? As this Part describes, in some cases, courts have held companies accountable for breaches of digital privacy, and they have achieved some degree of success in doing so, as the following discussion shows. At the same time, there are significant hurdles at present for the courts, acting on their own, to police digital privacy, especially when facing some of the immunities described in Part III. In this Part, I examine the relative success of the courts in achieving the policy goal of protecting digital privacy, and, by extension, political privacy.

A. Litigation Before the Cambridge Analytica Scandal

The primary avenue through which courts, on their own (that is, without some statutory claim), can protect digital privacy is through adjudication of disputes over tort actions for breaches of privacy.[216] While the privacy tort has been classified as really encompassing four torts,[217] the one that is most often implicated in disputes over violations of digital privacy is the tort of "intrusion upon seclusion."[218] The simplest and most common description of this tort is that it involves "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another" or that person's "private affairs or concerns," when such intrusion is "highly offensive to a reasonable person."[219] In the context of intrusions upon privacy on the internet, through apps, websites, or social media, courts have analyzed the technology that has been used by those who might intrude upon people's private matters to assess the extent to which an individual might have

215. *See infra* Part IV.

216. As a reflection of some of the impact of the immunities described in Part III, many of the plaintiffs' statutory claims in the cases described here have proven unsuccessful as vehicles for protecting digital and political privacy because such statutes, for the most part, are easily evaded by the defendants in these actions. *See supra* Part III.B. As Chander explains, while many of the relevant statutes have names that suggest they protect the consumer, they rarely do. *See* Chander, *supra* note 187, at 648-49, 666-67.

217. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

218. *See infra* notes 221-46 and accompanying text.

219. RESTATEMENT (SECOND) OF TORTS §625B (AM. LAW INST. 1977).

a reasonable expectation of privacy in the subject matter or the technology itself.[220] Much of this jurisprudence often hinges on whether the practice utilized by the potential tortfeasors is so widespread that it could not be said that the individual whose information was accessed or utilized could have reasonably believed it would be maintained as private. At the same time, courts have assessed the extent to which an individual may have chosen not to give consent to have his or her information accessed to gauge the degree of reasonableness of the intrusion.[221]

On one side of the ledger, courts have generally held that the use of tracking functions, often called "cookies," standing alone, does not constitute an unreasonable intrusion upon seclusion. One of the first cases to address this question involved the internet-based advertising company, DoubleClick,[222] an entity that Google would ultimately purchase.[223] That purchase would enhance Google's capacity to generate revenue through online advertising.[224] But when the issue of tracking cookies was first litigated, DoubleClick had a much less pervasive reach than the practice as it is embedded in most web-browsing functions today. In 2001, Doubleclick's tracking functions only occurred through websites affiliated with Doubleclick's advertising network, which, at the time, consisted of 11,000 websites.[225] Users that visited these websites had their activities on such sites tracked and might see banner advertisements on those sites based on their browsing activities.[226] Although the court would dismiss the plaintiffs' state claims without prejudice once it dismissed their federal claims,[227] the court's treatment of those federal claims can shed some light on how courts generally view claims about tracking software. For the court in *Doubleclick*, the practice of tracking online activities was carried out for commercial purposes and the defendant was quite transparent in its public filings about such practices.[228] Because of this transparency, the

220. *See, e.g.*, *In re* Facebook Internet Tracking Litigation, 263 F. Supp. 3d 836, 846 (N.D. Cal. 2017) (assessing reasonable expectation of privacy in sites Facebook users visited even when not using the Facebook application).

221. *See In re* Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 151 (3d Cir. 2015) (holding that a reasonable jury could conclude tracking of end users after they had explicitly indicated that they did not want to be tracked and company advertised that it respected such preferences "constitute[d] the serious invasion of privacy" under state law), *cert. denied sub. nom.* C.A.F. v. Viacom, 137 S. Ct. 624 (2017).

222. *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001).

223. Louise Story & Miguel Helft, *Google Buys DoubleClick for $3.1 Billion*, N.Y. TIMES (Apr. 14, 2007), https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html [https://perma.cc/VZH4-UPN4].

224. *Id.*

225. *DoubleClick*, 154 F. Supp. 2d at 502.

226. *Id.*

227. *Id.* at 526.

228. *Id.* at 518-19.

court found that the defendant did not have the requisite tortious intent for there to be liability for these actions.[229] Indeed, the defendant's purpose was not "to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites."[230] The court found further that "[i]f any of its practices ultimately prove tortious, then DoubleClick may be held liable for the resulting damage," but the court would conclude that the defendant did not have tortious intent in carrying out its business activities.[231] For the *DoubleClick* court, the pervasiveness of these commercial practices, engaged in by not just DoubleClick but many other entities at the time, could not be tortious or illegal because otherwise "[w]eb sites would commit federal felonies every time they accessed cookies on users' hard drives, regardless of whether those cookies contained any sensitive information."[232]

In a more recent case, the plaintiffs alleged that Facebook tracked internet users' online activity by "collecting detailed records of Plaintiffs' private web browsing history" by tracking the Uniform Resource Locators (or URLs) that the plaintiffs had visited if such URLs had Facebook's cookies embedded in them.[233] This activity extended to activities that took place even while the plaintiffs were logged out of Facebook.[234] The district court ultimately dismissed many of the plaintiffs' statutory claims on standing grounds, but proceeded to assess their tort claims based on invasion of privacy and intrusion upon seclusion, finding that with such claims, the plaintiffs need not allege a tangible, pecuniary harm from a privacy violation to have standing.[235] Turning to the merits of the plaintiffs' privacy claims, the court's decision to dismiss those claims hinged on whether the plaintiffs had a reasonable expectation of privacy in the URLs that they visited in the internet, which, in turn, depended on whether those plaintiffs had taken steps to block their internet activity from tracking. As the court found, "[p]laintiffs have not established that they have a reasonable expectation of privacy in the URLs . . . they visit" because they "could have taken steps to keep their browsing histories private" either by removing, blocking, or preventing the transmission of information to third parties by adjusting their individual browser settings.[236] The court also found that the type of activity and information that was being tracked by Facebook and transmitted to third parties was precisely

229. *Id.* at 519.

230. *Id.*

231. *Id.*

232. *Id.* at 513.

233. *In re* Facebook Internet Tracking Litigation, 263 F. Supp. 3d 836, 840 (N.D. Cal. 2017).

234. *Id.*

235. *Id.* at 843.

236. *Id.* at 846.

the types of data that are routinely utilized by entities involved in internet communications. These activities were thus "part of routine internet functionality and can be easily blocked,"[237] therefore the monitoring and transmittal of such information did not constitute a " 'highly offensive' invasion of Plaintiffs' privacy interests."[238]

But on the other side of the ledger are more recent opinions that reveal a tension within the jurisprudence on the legality of tracking software. An important 2015 opinion from the U.S. Court of Appeals for the Third Circuit involved litigation regarding Google's disregard of user preferences with respect to online tracking.[239] In that case, users of Google services had expressed their desire to opt out of having their online activities tracked by using a "cookie blocker" which, theoretically, would prevent Google from utilizing cookies to monitor these users' online behavior.[240] Google had advertised that it honored these efforts to insulate these users from efforts to track their digital activities.[241] In reality, Google had, indeed, engaged in tracking of these users' activities.[242] While the Court of Appeals affirmed the dismissal of several statutory claims, it overturned the lower court's rulings regarding the state common law and constitutional privacy claims under California state law, holding that "Google not only contravened the cookie blockers—it held itself out as respecting the cookie blockers."[243] The court found that "[w]hether or not data-based targeting is the internet's pole star, users are entitled to . . . rely on the public promises of the companies they deal with."[244] Making matters worse, the court found that Google's behavior was "broad" because it "touch[ed] untold millions of internet users[,] . . . was surreptitious[,] . . . [and] of indefinite duration."[245] Because of these findings, the court concluded that "a reasonable factfinder could indeed deem Google's conduct 'highly offensive' or 'an egregious breach of social norms,' " such that the court would overrule the district court's dismissal of the state-based privacy claims.[246] Similarly, while the same court as that which reached the *Google* decision—the Third Circuit—recognized that the use of track-

237. *Id.*

238. *Id. See also* Van Patten v. Vertical Fitness Grp., 847 F.3d 1037, 1043-45 (9th Cir. 2017) (holding no violation of law regarding contact through text messages when plaintiff consents to receipt of such messages).

239. *In re* Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 126 (3d Cir. 2015).

240. *Id.* at 131.

241. *Id.* at 132.

242. *Id.* at 132-33.

243. *Id.* at 151.

244. *Id.*

245. *Id.*

246. *Id.* at 151-53.

ing mechanisms themselves might not constitute outrageous conduct,[247] even when used on children through a website geared towards children.[248] At the same time, when another company, Viacom, promised parents that it would not track their children's activities while they were on the company's site (even though it did, in fact, track that activity), this "may have encouraged parents to permit their children to browse those websites under false pretenses."[249] As a result, this led the court to find that "a reasonable jury" could conclude that such acts might constitute a tortious intrusion upon seclusion.[250]

What this review of these emerging cases reveals is that there is a divide in the jurisprudence around digital tracking. Courts acknowledge that much tracking is completely acceptable, partly because it is so ubiquitous and widespread.[251] As a result, courts are asking how can something that occurs so frequently be outrageous to such an extent that it would satisfy the tort standard? Moreover, even if some tracking may seem inappropriate, where an individual consents to permit such tracking, the entity that secured that consent is also immune from tort liability. Thus, we can read into the institutional response—that is, the response from the courts—to intrusions upon digital seclusion the notion that the behavior of market actors, when unchecked by the political process, can have profound influence on the willingness of the courts to rein in actions that affect digital, and by extension, political privacy.

At the same time, it appears that courts, independent of the action or inaction of other institutional settings to intervene to protect political privacy, are beginning to scrutinize the consents contained in terms-of-service agreement to ensure that they are clear and cover the entity's behavior. What is more, if there is some deception or fraud, like the entity promises that it will not track such activity and does, courts have found it appropriate to permit claims that the behavior constitutes an intrusion upon seclusion.

While many of these results address digital privacy more broadly, they have clear ramifications for political privacy. An exploration of how to build upon them to strengthen the capacity of private-law protections to preserve the integrity of individual and collective identity follows in the last and final Part. How these forces are playing out in one setting—the litigation over the Cambridge Analytica scandal—where political privacy is directly implicated, helps set the stage for that larger discussion of institutional responses to the policy problem of protecting political privacy. It is to that litigation that I turn next.

247. *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 294 (3d Cir. 2016).

248. *Id.* at 294-95.

249. *Id.* at 295.

250. *Id.*

251. *See supra* notes 225-32 and accompanying text.

B. The Cambridge Analytica Litigation

Facebook has faced challenges to a wide range of its practices similar to the lawsuits described above, from allegations that it tracked its users' web-browsing activities even after the users left Facebook[252] to its use of facial-recognition software and storage of facial-recognition data without users' consent.[253] Most recently, and most germane to this discussion, Facebook has faced litigation for the Cambridge Analytica scandal itself described above.[254] There, plaintiffs have alleged that not only did Facebook share private information with Cambridge Analytica and other third parties but also that such information was "substantive and revealing," including "photographs, videos [plaintiffs] made, videos they watched, their religious and political views, their relationship information, and the actual words contained in their messages."[255]

Facebook presented various defenses in this action and the court readily dismissed the first of these. The court described that defense as follows:

> Facebook argues that people have no legitimate privacy interest in any information they make available to their friends on social media. This means, according to Facebook, that if people use social media to communicate sensitive information with a limited number of friends, they have no right to complain of a privacy violation if the social media company turns around and shares that information with a virtually unlimited audience.[256]

The court responded that "Facebook's argument could not be more wrong,"[257] noting that "[w]hen you share sensitive information with a limited audience (especially when you've made clear that you intend your audience to be limited), you retain privacy rights and can sue someone for violating them."[258] The court went on to review a range of practices utilized by Facebook with respect to user information, including sharing it with groups like Cambridge Analytica; not monitoring the use and abuse of such information by third parties who gained access to it; sharing a wide range of personal information with preferred third parties; and giving access to not just users' information who might interact with a third-party app developer but also information

252. *In re* Facebook Internet Tracking Litig., 263 F. Supp. 3d 836, 840 (N.D. Cal. 2017).

253. Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct 937 (2020).

254. *In re* Facebook, Inc., Consumer Privacy User Profile Litig., 402 F. Supp. 3d 767, 776 (N.D. Cal. 2019).

255. *Id.* at 776.

256. *Id.* at 776. The argument is more fully described later in the court's opinion. *See id.* at 782.

257. *Id.* at 776.

258. *Id.*

related to the private information of those users' personal networks.[259] Facebook was also giving access to information from the accounts of friends of those users when the users gave them consent to do so, even though the company never obtained direct consent from those friends in any way.[260] With respect to the last item, which occurred in the Cambridge Analytica scandal, the court described how broad such access could be: even though an app developer who would ultimately share his information with Cambridge Analytica gained direct access to only 300,000 Facebook users who interacted with his app, he was nevertheless able to "compile a database with information on roughly 87 million Facebook users," by obtaining access to the individuals on the private "friend" networks of those initial 300,000 individual users.[261]

As with other cases, the question of whether the plaintiffs had standing, or could claim they were harmed in any way by these practices, was at the center of the court's decision; in turn, whether the plaintiffs could claim standing and allege that they were harmed hinged on whether they consented to the practices about which they were complaining.[262] The court would find that "[i]n privacy cases, the standing and merits inquiries will often be intertwined . . . . [T]he extent to which you have a reasonable expectation of privacy relates not only to whether you've stated a claim for invasion of privacy but whether you were injured by the invasion in the first place."[263]

The court then analyzed whether the plaintiffs had consented to the four different practices at the center of the suit and found that with most of them, the plaintiffs had not consented to those practices: for example, sharing private information with particular business partners of Facebook, sharing with "whitelisted apps," and failing to prevent misuse.[264] With the fourth category, giving access to the users' networks, the issue of consent was not so clear. Facebook's terms of service provisions after 2009 seemed to indicate that anything a user shared with his or her network could, in turn, be shared by the individuals in that network with third parties, " 'including the games, applications, and websites they use.' "[265] A provision in Facebook's Data Use Policy did, indeed, say that a user could " 'completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications.' "[266] Doing

259. *Id.* at 779-81.
260. *Id.*
261. *Id.* at 780.
262. *Id.* at 787-95.
263. *Id.* at 788.
264. *Id.* at 792-95.
265. *Id.* at 792 (citing Facebook's Data Use Policy).
266. *Id.*

so, however, would mean that the user would " 'no longer be able to use any third-party Facebook-integrated games, applications, or websites.' "[267]

The court would ultimately find that those individuals who joined Facebook after 2009 were subject to this provision with respect to this type of information and thus consented to third-party access to their information through their networks if they did not follow the protocols set forth in the Data Use Policy to block such access.[268] At the same time, if a plaintiff had joined Facebook prior to 2009 when these protocols were put into place, the court found they had not consented to such practices.[269] While the court recognized that a layperson would not generally have understood the provisions in the Data Use Policy, users subject to the 2009 update "who did not properly adjust their application settings [were] deemed to have agreed that app developers could access their information."[270]

While lawsuits over digital privacy will no doubt continue to emerge, what we know of the results of the decisions courts have issued to date in this area can help us understand the need for a multidimensional approach to protecting political privacy, one that I will explore in subsequent parts. As the preceding discussion shows, the courts have proven effective, to a certain extent, and certainly when compared to the other institutional settings described here, in protecting political privacy, but the role of the courts has been significantly diminished by barriers to achieving such protection imposed by those other institutions. First and foremost, the private sector has succeeded in many respects in insulating the actions of digital actors from judicial review through such mechanisms as terms-of-service agreements that require consumers to consent to the sharing of private information as a condition of receiving service from the companies and/or require customers to accept mandatory arbitration for the resolution of disputes. For these reasons, the ability of courts to serve as an effective outlet for the protection of digital privacy is limited to say the least. At the same time, Congress has created barriers to the aggressive policing of political privacy violations, both procedural and substantive, including passing legislation that honors arbitration clauses except in extreme circumstances and grants internet platforms immunity from liability for content on such platforms. Congress has also failed to pass effective legislation to protect political privacy, as many of the statutory challenges that litigants have brought have proven, for the most part, unsuccessful. While some litigants have progressed through the courts and achieved some degree of success, the judicial

267. *Id.*

268. *Id.*

269. *Id.* at 793-94.

270. *Id.* at 792-93.

setting will always have its limitations, unless more is done in an integrated fashion across the three institutional settings to enhance and preserve digital privacy. The following section explores what such an integrated, multi-institutional approach to enforcing digital privacy might look like.

V. AN INTEGRATED, MULTI-DIMENSIONAL APPROACH TO PROTECTING DIGITAL PRIVACY

What the previous two parts showed is that, first, the courts have proven somewhat constrained by the fact that market forces and legislative action and inaction have created immunities that make it more difficult to prosecute political privacy violations. Second, and also a reflection of the first phenomenon, is that different institutional settings, operating independently, might be in weaker positions than they would if they coordinated and cooperated in the development of effective approaches towards protecting political privacy. Furthermore, advances in technology make it difficult for law to catch up with them and to secure protections for the use and abuse of technology.[271] When we appreciate these three phenomena, we realize that an integrated, comprehensive, cooperative, and agile model of oversight might prove the most effective in protecting and preserving political privacy. In some ways, such an approach will have to combine the agility of markets with the accountability the judicial system offers—with government efforts playing an essential oversight role as well. Such an approach would combine the following. First, consumer education as to the risks posed to consumers' personal, private information; once the consumer knows of these risks, this raises the stakes as to those consumers' legitimate expectations of privacy and the intrusion upon such private matters is more egregious. Second, it would entail clear and appropriate disclosures of the practices of any entity that has possession of or access to that individual's private information. Third, there would be robust accountability provisions allowing easy, effective, and efficient access to the courts for breaches of this private information. I will discuss each of these components, in turn, below.

A. The Components of an Institutionally Integrated Regime for Protecting Political Privacy

1. Consumer Education and Public Awareness

Consumer education is a critical aspect of preserving the integrity of identity. A now-famous line, attributed to Scott McNealy of Sun Microsystems, may capture how Silicon Valley thinks about consumer

271. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196-97 (1890). The origins of the current conception of the right to privacy can be traced to the authors' fear that technology was outpacing the law existing at the time.

privacy: "You have zero privacy anyway . . . [g]et over it."[272] That does not mean that courts must accept this position. A recent study conducted by Pew Research Center revealed that Americans are greatly concerned about the privacy of their online activities and those carried out through mobile technologies and applications.[273] At the same time, most Americans are concerned that such information is being used by private industry and the government.[274] When it comes to accepting policies affecting digital privacy, ninety-seven percent of those surveyed by Pew stated that they are asked to accept such policies, but only nine percent claim that they always read such policies and another thirteen percent say that they often read such policies.[275] A full thirty-six percent said they never read such policies before accepting them,[276] a number which, according to other research, would seem quite low.[277] What is more, according to Pew, "72% of Americans report feeling that all, almost all or most of what they do online or while using their cellphone is being tracked by advertisers, technology firms or other companies."[278] Finally, seventy-nine percent of those surveyed said that they are either "not too or not at all confident that companies will admit mistakes and take responsibility if they misuse or compromise personal information."[279]

There is a bit of a paradox in the relationship between consumer knowledge and threats to the integrity of identity in that if one does not know one's personal information is under threat then it is unlikely that at least some of the negative externalities associated with intrusion upon one's personal seclusion will come to pass.[280] If I do not know that I am being surveilled, then I will not curtail my activities in any way and it will not chill my speech or actions.[281] What is more, as I learn a greater amount about the threats to the integrity of my individual and collective identity, the more likely it is that such negative

272. Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED MAG. (Jan. 26, 1999, 12:00 PM), https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ [https://perma.cc/9DWR-ZBN5].

273. BROOKE AUXIER ET AL., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION, PEW RESEARCH CTR. 2 (2019).

274. *Id.*

275. *Id.* at 5.

276. *Id.*

277. Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 605 (2014) (noting results of experiment where seventy-seven percent of respondents did not review contract terms prior to accepting them).

278. AUXIER, *supra* note 273, at 6.

279. *Id.* at 4.

280. *See* TUFECKI, *supra* note 67, at 224-26 (discussing role of knowledge of privacy breach has to harms associated with that breach).

281. *But cf.* Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring) (noting intrusions of which the victim is unaware are potentially more harmful than intrusions of which that individual is aware).

externalities from such threats will arise.[282] Thus, while it can be argued that one has to know that one's seclusion is being intruded upon for there to have been an intrusion upon it and for the negative effects to come about, and that the more one knows of such threats to one's privacy the greater the potential chilling effect,[283] nevertheless, raising awareness about such threats has potential and significant downstream effects in terms of balancing out the asymmetry of information related to such threats that enables them to arise in the first place.[284] What is more, knowledge about such threats empowers consumers to take action to prevent against them and to act, where possible, to ensure they are not unwittingly providing consent to such widespread data practices. Of course, consumer education alone, without improved disclosures and clearer means by which consumers can withhold their consent is meaningless. As a result, improved disclosures are a necessary complement to consumer education, as the following section argues.

2. *Improved Disclosures*

As described above and as we have seen in recent litigation around the exploitation of digital information, many intrusions upon such information are entirely legal in the sense that consumers have signed away their rights to such information.[285] Indeed, inadequate disclosure of contract provisions through opaque terms-of-service agreements is standard practice in the digital world.[286] And acceptance of such terms is often the price of admission into the digital world and mandatory.[287] What is more, asymmetry in consumer knowledge about the terms they are accepting means many consumers are unaware of the rights

282. *See, e.g.*, Hirsch, *supra* note 195, at 71-74 (describing some of the negative externalities of privacy violations).

283. Ellsberg v. Mitchell, 709 F.2d 51, 67 n.71 (D.C. Cir. 1983) (in the Fourth Amendment context noting "awareness that one's conversations may be being overheard and recorded is likely to have a chilling effect on one's willingness to speak freely"), *cert. denied sub nom.* Russo v. Mitchell, 465 U.S. 1038 (1984).

284. Of course, greater awareness of risk is not always a panacea that brings about better decisionmaking. OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 64-66 (2014) (describing shortcomings in disclosure regimes). For suggestions for how to overcome some of these shortcomings, see Lauren E. Willis, *Performance-Based Consumer Law*, 82 U. CHI. L. REV. 1309, 1330-45 (2015).

285. Nancy Kim has argued that such use of contract law does not just protect one party but also divests the counter-party of rights. KIM, *supra* note 175, at 48-49.

286. *See, e.g.*, LAWRENCE LESSIG, THEY DON'T REPRESENT US: RECLAIMING OUR DEMOCRACY 212-14 (2019) (describing consent practices).

287. BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 210 (2018). Indeed, when faced with terms of service agreements, acceptance of such terms is the norm: "Deliberation is wasteful. . . . Resistance is futile." *Id.* On technological determinism generally, see Wei Lu, *From Determinism to Interaction: Building a New Model of Technological Evolution*, *in* CULTURAL ATTITUDES TOWARDS TECH. AND COMM. 2004: PROC. OF THE FOURTH INT'L CONF. ON CULTURAL ATTITUDES TOWARDS TECH. & COMM. 614-24 (2004).

they are surrendering as they utilize digital services and enter the digital world.[288] As Lawrence Lessig explains: "[p]rivacy law and online practices have assumed that if the lawyers can bury the permission in a click-wrap terms of service, then all bets are off."[289]

New rules that apply to the European Union and in the state of California may curb some of these practices,[290] and such rules may become the de facto new rules for the internet and mobile technologies.[291] Disclosure alone, if it is not accessible and understandable, will not overcome the immunity many service providers enjoy when they exploit digital information.[292] At the same time, disclosures that are easy to understand and mandatory, which require entities with access to private information to disclose the fact of their access and how they intend to use such information, should be required of any entity seeking to utilize individual data.[293] When coupled with greater public awareness about the risks inherent in providing access to personal information and guidance about how the individual can protect herself from the risk of such access, simple, easy-to-understand disclosures can help overcome information asymmetries surrounding data access and abuse.[294] At the same time, entities will often find ways to undermine disclosure regimes and bend them to their interests.[295] While disclosure is important and employing simple and easy-to-understand disclosures can help overcome the barriers to consumer appreciation for the risks inherent in the practices of which they plan to engage, it

288. RADIN, BOILERPLATE, *supra* note 180, at 7-16 (describing the asymmetries of information between consumers and companies).

289. LESSIG, *supra* note 286, at 213.

290. For an analysis of these new disclosure standards, see generally Rustad & Koenig, *supra* note 12, at 365.

291. For a description of the Microsoft Corporation's efforts to comply with the European Union's new privacy rules, which entailed reforming all of their practices, not just those directly covered by European Union regulations, see SMITH & BROWNE, *supra* note 11, at 139-41.

292. *See* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 665-71 (2011) (arguing disclosure is generally ineffective in many consumer settings).

293. *See* Ayres & Schwartz, *supra* note 277, at 579-89 (arguing that clearer and simpler disclosures can overcome information asymmetries); John Kozup et al., *Sound Disclosures: Assessing When a Disclosure is Worthwhile*, 31 J. PUB. POL'Y & MARKETING 313, 315-17 (2012) (arguing message format and simplicity can impact consumer understanding); Vanessa G. Perry & Pamela M. Blumenthal, *Understanding the Fine Print: The Need for Effective Testing of Mandatory Mortgage Loan Disclosures*, 31 J. PUB. POL'Y & MARKETING 305, 307 (2012) (same).

294. Ben-Shahar & Schneider, *supra* note 292, at 743-47. Another note of caution—disclosure may affect outsider perspectives disproportionately, further chilling associational activity. *See* Leslie Kendrick, *Disclosure and Its Discontents*, 27 J.L. & POL. 575, 595 (2012) (cautioning that "[o]ne feature of disclosure regulations is that they are likely to have a disparate impact on unpopular views") (footnote omitted).

295. *See, e.g.*, SUNSTEIN, *supra* note 181, at 109 (describing the manipulation of default options that include disclosures).

is not perfect, which means we will need even further enhanced protection, through both ex ante legislative and regulatory protections and ex post tort liability, which go beyond mere disclosure, as the following sections argue.

One type of robust, yet simple, disclosure regime could involve what I have proposed elsewhere as a form of "digital zoning."[296] Such an approach would borrow from property law contexts—like zoning in the physical world, restrictive covenants, and mortgage disclosure rules—that could enable individuals to understand the types of protections and the extent to which the information that is gathered and shared over the internet and through mobile technologies is protected or exposed. Such a system would require sites and apps to disclose things like what type of information they glean from their customers and the ways the companies use such information. Such companies would also have to reveal whether they share such private information with third parties and, if they do, they will also have to disclose how those third parties are using such information as well. Similarly, they would have to disclose whether disputes with such customers are covered by arbitration clauses, among other matters.[297] And this last point leads to a larger point: even with these protections, we would still need robust, transparent, and accountable enforcement measures—in other words, we still need courts.

3. Utilization of the Courts

The preceding discussion about the courts should reveal several things about ex post interventions to punish violations of political privacy. First, they do seem to offer stronger protections than exist through just the market or the political process. Second, and importantly, they are interdependent with those other institutional settings. That is, the courts do not operate in a vacuum to protect political privacy. The market has proven effective in developing immunities from liability for privacy violations, the strongest of which is the protection—through contract—of providers that share private information with third parties. Similarly, the political process has generated immunities of its own, by passing legislation that insulates providers from liability for the actions of third parties on internet platforms. The market and the political process can also work together to protect providers, as when contracts contain mandatory arbitration clauses and legislation requires courts to honor them. The courts have demonstrated that they can serve as a robust arena—at least relatively speaking, when compared to the other institutional settings—for the protection of political privacy. But, as we have seen, the courts

296. *See* Brescia, *Zoning Cyberspace*, *supra* note 74.

297. *See id.* at 1244.

are often powerless in the face of other institutions when those institutions create barriers that impede the effective adjudication of privacy disputes. In other words, we have to be sensitive to the fact that private and political institutions can undermine the courts' effectiveness should they attempt to serve as defenders of digital privacy. Thus, the three institutional systems are integrated, and the action or inaction of one system can have lasting and spillover effects on another system's capacity to protect digital, and, in turn, political privacy.

B. The Problem of Political Privacy and What It Reveals about Comparative Institutional Analysis

The susceptibility of courts to the efforts of other institutional settings to encroach upon judicial efforts to protect political privacy reveals the interdependence of institutions in the protection of such privacy and reinforces the notion that some institutional settings can have negative spillover effects on others. Of course, they can also have positive spillover effects, as when legislators and regulators limit the extent to which mandatory arbitration clauses are enforceable, or where they prohibit privacy-undermining practices. It also points to the need to incorporate protections for political privacy, from different institutional settings, that recognize the ways in which those settings can have positive and negative effects on the ability to secure desired policy goals. This points to the inherent interdependence of institutional settings, at least with respect to complex problems and complex policy goals, like the need to protect political privacy. Thus, this discussion reveals not just the nature of the problem and the need for a particular kind of institutional analysis and institutional response, it also exposes something else: the nature of comparative institutional analysis itself, the idea that institutional settings—identified as the market, the political process, and the courts—are not monolithic, nor do they operate independently of one another. This insight has implications for achieving the goal of protecting political privacy, for certain, but it also enriches our understanding of institutions and the methods of conducting comparative institutional analysis to yield desired policy goals. When utilizing this methodology to identify the proper institutional setting in which and through which to achieve a policy goal, one needs to appreciate the extent to which other institutional settings may enhance, or undermine, the efforts to achieve that goal. Thus, any effective comparative institutional analysis must respect and recognize the extent to which, in a particular policy setting, different institutions operate in an interdependent fashion.

CONCLUSION

There are few concepts of greater importance in a democracy than political privacy. It is central to the preservation of autonomy and the

realization of self-determination. It is also critical to social engagement and social change—the tools of self-determination. We largely protect political privacy from government intrusion through public-law means: constitutional and statutory protections that rein in government actors. At the same time, today, with the diffusion of digital and mobile technologies, some of the greatest threats to political privacy come from private entities beyond the reach of many of these public-law protections. With private-law protections, however, it is easy for different institutional settings to create conditions in which this political privacy is undermined. Those different institutional settings can have spillover effects on the functioning of other institutions, meaning we cannot conduct either an analysis of just one institution or even compare institutions against each other to find the best institution through which to regulate political privacy. Distortions, through capture, self-interest, rent-seeking, and other forces, can result in the weakening of one institution's response to political privacy. These distortions can, in turn, affect the functioning of other institutions. Thus, not only is it difficult to conduct single institutional analysis, but it is also challenging to conduct comparative institutional analysis without an appreciation for the extent to which institutions can have effects outside their individual institutional settings. What this means is that, at least with respect to achieving the desired policy goal of protecting political privacy, we must appreciate the ways in which the institutional settings that might regulate political privacy are interdependent and require an approach to these institutions that embraces, rather than ignores, that interdependency. This Article has been a modest attempt to do just that: to consider ways that a cooperative, cross-institutional approach to protecting political privacy is the best way to secure such protections.