Note

It's the Autonomy, Stupid: Political Data-Mining and Voter Privacy in the Information Age

*Chris Evans**

INTRODUCTION

Imagine American democracy without the secret ballot. Candidates could effectively bribe and otherwise coerce voters. Voters themselves would feel social pressure to vote against dissenters and unpopular ideas. Minority viewpoints would struggle to gain traction. Such was the state of elections in the United States through most of the nineteenth century, prior to widespread adoption of the secret ballot.[1] By the turn of the twentieth century, Progressives had successfully advocated for introduction of the secret ballot "to enhance citizen independence and sincerity by freeing voters to vote their actual preferences rather than those of a party to which they felt beholden or that they feared."[2] In theory, voters would be free to exercise their basic democratic right autonomously and out of view of the party bosses.[3]

Information Age political tactics are unraveling the anonymity afforded by the secret ballot. To more effectively target voters, campaigns have become voracious collectors of personal data.[4] Databases operated by the major political parties as well

* J.D. Candidate, University of Minnesota Law School. Chris would like to thank Professor McGeveran for his guidance and the editors and staff of the Journal for their improvements to this Note.

1. James A. Gardner, *Anonymity and Democratic Citizenship*, 19 WM. & MARY BILL RTS J. 927, 943 (2011) ("The principal justification for introducing the secret ballot, a reform backed strongly by Progressives, was to break the control that parties were thought to exercise over voters by depriving them of the ability to enforce discipline at the polls.").

2. *Id.*

3. *Id.*

4. *See, e.g.*, Micah Sifry, *How Obama's Data-Crunching Prowess May Get Him Re-Elected*, CNN.COM (Oct. 9, 2011), http://www.cnn.com/2011/10/09/tech/innovation/obama-data-crunching-election/index.html?hpt=hp_c2 (describing

as by candidates and consultants contain information gleaned and purchased from public and private sources on nearly every voter in the United States.[5] The goal of these "digital dossiers"[6] is to profile likely voters and identify traits that predict voting habits.[7] Political data-mining has proven to be a winning election tactic, but the resulting erosion of voter privacy has gone unabated. Although voters still enjoy privacy once they enter the voting booth, their movements outside the polling place are cataloged to an extent that may defeat the purpose of secret balloting.[8]

This Note will explore the unique threats to the right to privacy posed by political data-mining. Section I explicates modern privacy law and details the process of data-mining. Section II examines how political campaigns use data-mining and how political data-mining poses unique threats to privacy. Section III looks at potential approaches to protecting privacy from political data-mining and recommends that the United States adopt a voter data disclosure law that allows voters to see what data campaigns maintain about them and gives voters the option of opting out of profiling.

---

the campaign's success at the "modern mechanics of identifying, connecting with and mobilizing voters, as well as the challenge of integrating voter information with the complex internal workings of a national campaign").

5. James Verini, *Big Brother Inc.*, VANITY FAIR, Dec. 2007, *available at* http://www.vanityfair.com/politics/features/2007/12/aristotle200712?printable=true&currentPage=all ("Aristotle's massive private database contains detailed information about roughly 175 million American voters."); *see also* Garrett M. Graff, *They Have Your Number*, THE WASHINGTONIAN, Oct. 1, 2008, at 48 *available at* http://www.washingtonian.com/print/articles/6/171/9627.html (noting that the Catalist database "contains some 280 million individual records").

6. "[D]igital dossiers are increasingly becoming digital biographies, a horde of aggregated bits of information combined to reveal a portrait of who we are based upon what we buy, the organizations we belong to, how we navigate the Internet, and which shows and videos we watch." DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 168 (2004) [hereinafter SOLOVE, DIGITAL PERSON].

7. Leslie Wayne, *Voter Profiles Selling Briskly as Privacy Issues Are Raised*, N.Y. TIMES, Sept. 9, 2000, at A10 ("[S]uch precise information is golden, enabling them to identify potential supporters and not waste money on the unswayable.").

8. "Development of the capacity for autonomous choice is an indispensable condition for reasoned participation in the governance of the community and its constituent institutions—political, economic, and social." Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000) [hereinafter Cohen, *Examined Lives*].

I. BACKGROUND

A. THE RIGHT TO PRIVACY

When Warren and Brandeis wrote "The Right to Privacy" in 1890, they were responding to technological advancements and newspaper enterprises that "threaten[ed] to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[9] They argued the law should recognize and protect the individual's privacy, separate from existing slander, contract, and other laws.[10] Seventy years later, William Prosser surveyed the still unsettled privacy landscape and identified four separate torts comprising the right to privacy: 1) intrusion of solitude; 2) public exposure of private facts; 3) false light publicity; and 4) appropriation of name or likeness.[11] Courts today recognize all four of these torts, and many states have codified them.[12] But as advancing technology changes the way individuals keep information to themselves or share it with others, legal scholars continue to struggle to de-

---

9. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

10. *See id.* at 197.

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

12. Intrusion of solitude (or upon seclusion) has three elements: "(1) an intrusion; (2) that is highly offensive; and (3) into some matter in which a person has a legitimate expectation of privacy." Swarthout v. Mutual Service Life Ins. Co., 632 N.W.2d 741, 744 (Minn. Ct. App. 2001) (holding that illicitly obtaining a patient's medical records may be a breach of privacy). Public exposure (or disclosure) of private facts occurs when "[p]ublicity [is] given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person." Pachowitz v. LeDoux, 666 N.W.2d 88, 94 (Wis. Ct. App. 2003) (holding that disclosure of a patient's medical condition by an emergency medical technician to a coworker could constitute an invasion of privacy claim). A claim of false light publicity requires "publicity to a matter concerning another that places the other before the public in a false light" that "would be highly offensive to a reasonable person." Welling v. Weinfeld, 866 N.E.2d 1051, 1059 (Ohio 2007) (holding false light publicity to be an actionable tort in Ohio); *see also* DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 24–25 (2003) ("The states have passed statutes protecting privacy in many contexts . . . from employment records and medical records to library records and student records."); c*f.* Denver Pub. Co. v. Bueno, 54 P.3d 893, 894 (Colo. 2002) (declining to recognize false light publicity as a tort separate from defamation). A person may be liable for a breach of privacy when he appropriates another person's name or likeness "to his own use or benefit." Remsburg v. Docusearch, Inc., 149 N.H. 148, 157 (N.H. 2003) (quoting RESTATEMENT (SECOND) OF TORTS § 652C at 380) (explaining that personal information sold for the value of the information itself is not an actionable appropriation).

fine "privacy."[13]

A key theoretical difficulty with defining the right to privacy is the overlapping areas of law that protect what we think of as privacy.[14] The Constitution protects citizens from breaches of privacy by the government through the First, Fourth, and Fifth Amendments.[15] The Supreme Court has also recognized that the Bill of Rights casts "penumbras" which create certain "zones of privacy" into which the government may not intrude.[16] Breaches of privacy by nongovernmental entities fall under the privacy torts or state and federal statutes.[17] A person who sexually harasses a coworker has violated the coworker's privacy,[18] and an employee who breaks a confidentiality agreement breaches his employer's privacy.[19] Neither case fits

---

13. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477–48 (2006) [hereinafter Solove, *Taxonomy*]. ("Privacy is far too vague a concept to guide adjudication and lawmaking, as abstract incantations of the importance of 'privacy' do not fare well when pitted against more concretely stated countervailing interests.").

14. *See, e.g.* Smith v. Stewart, 660 S.E.2d 822, 834 (Ga. Ct. App. 2008) (holding plaintiff's false light privacy claim to be encompassed in her defamation claim); *see also* YAEL ONN ET AL., HAIFA CTR. OF LAW AND TECH., PRIVACY IN THE DIGITAL ENVIRONMENT 2–4 (2005); Solove, *Taxonomy*, *supra* note 13, at 483 (noting that American privacy law "extend[s] beyond torts to the constitutional 'right to privacy,' Fourth Amendment law, evidentiary privileges, dozens of federal privacy statutes, and hundreds of state privacy statutes").

15. U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech, or of the press."); U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."); U.S. CONST. amend. V ("nor shall private property be taken for public use, without just compensation."); *see also* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding "that the Fourth Amendment draws 'a firm line at the entrance to the house'"); Katz v. United States, 389 U.S. 347, 351 (1967) (noting that what information a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected"); SOLOVE, DIGITAL PERSON, *supra* note 6, at 62–64.

16. Griswold v. Connecticut, 381 U.S. 470, 484 (1965).

17. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681(a)(4) ("There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."); Gramm-Leach-Bliley Act of 1999, 15 U.S.C § 6802 (2006) (restricting financial institutions' use of consumers' personal information).

18. JEFFREY ROSEN, THE UNWANTED GAZE 15 (2000) ("The sexual harassment cases . . . may be better conceived as invasions of privacy.").

19. Pepsico, Inc. v. Redmond, 54 F.3d 1262, 1271 (7th Cir. 1995) (sustaining an injunction because employee's job would require disclosure of trade secrets protected by a confidentiality agreement).

neatly within the privacy torts of intrusion on solitude or public disclosure of private facts, but both are apparently breaches of privacy. Sexual harassment statutes exist to govern the first case, and the law of contracts exists for the second. But other exposures of private facts and intrusion on solitude fall outside the privacy torts, contract law, and statutes yet still breach privacy.[20] Privacy often exists in the negative space between laws, making it difficult to define.

1. Limitations to the Right to Privacy

The right to privacy has been defined broadly as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others,"[21] but observers have identified several limitations. Among those limitations, some argue that information involving the public interest should not be suppressed by privacy laws.[22] Warren and Brandeis argued privacy was not breached by disclosures in "court[s] of justice, in legislative bodies, or the committees of those bodies" or in other public bodies.[23] They also would exempt oral disclosures of private information from privacy law.[24] Once an individual consents to publish private facts, he loses his right to privacy in those facts.[25] The privacy torts generally only protect information that would be "highly offensive" to a reasonable person.[26] The Constitution "protects people, not places,"[27] but constitutional protections against governmental breaches of privacy generally do not extend to public spaces, nor do they restrict invasions of privacy by private parties.[28] Warren and Brandeis recommended damages and injunctive relief as remedies for breaches of privacy, but were more skeptical of levying

---

20. *See, e.g.*, SOLOVE, DIGITAL PERSON, *supra* note 6, at 81 ("Although contract law can protect privacy within relationships formed between parties, it does not redress privacy invasions by third parties outside of the contractual bonds.").

21. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

22. Warren & Brandeis, *supra* note 9, at 215.

23. *Id.* at 216.

24. *Id.* at 217.

25. *Id.* at 218.

26. *See supra* note 12.

27. Katz v. United States, 389 U.S. 347, 351 (1967).

28. *See, e.g.*, United States v. Knotts, 460 U.S. 276 (1983) (holding that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

criminal sanctions.[29]

The rights of private entities who breach privacy interests frequently outweigh the rights of the party whose privacy has been breached.[30] Particularly in cases of political speech, courts balance the right to privacy against free speech and the free flow of information—and privacy usually loses.[31] The First Amendment protects political speech above all other speech, but certain expressive activity falling under that protection breaches privacy.[32] However, privacy may outweigh free speech interests if speech about private information is considered to hold a lower value than speech about public information.[33]

2. Privacy-Related Harms

Defamation, slander, breaches of confidentiality agreements, sexual harassment, identity theft, intentional infliction of severe emotional distress are all causes of action that describe invasions of privacy, but they do not fully describe the nature of privacy or the nature of the harm when privacy is breached.[34] Warren and Brandeis wrote of the necessity of

---

29. Warren & Brandeis, *supra* note 9, at 219–20.

30. *See, e.g.*, William McGeveran, *Mrs. McIntyre's Persona: Bringing Privacy Theory to Election Law*, 19 WM. & MARY BILL RTS. J. 859, 860 (2011) ("High Court rulings since [McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995)] have consistently upheld disclosure requirements in election law.").

31. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Talking About You*, 52 STAN. L. REV. 1049, 1051 (2000) ("While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law."); s*ee, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 528 (2001) (holding individuals' privacy interest in illegally-recorded conversations did not justify proscribing broadcast by the media); Cohen v. California, 403 U.S. 15, 21 (1971) ("The ability of government, consonant with the Constitution, to shut off discourse solely to protect others from hearing it is, in other words, dependent upon a showing that substantial privacy interests are being invaded in an essentially intolerable manner."); *see also* Raymond T. Nimmer, *"Privacy" and "Data Protection" Defined—"Data Protection" as a Contrasting Idea*, *in* THE LAW OF COMPUTER TECHNOLOGY 17:5 (4th ed. 2011).

32. *See, e.g.*, *Cohen*, 403 U.S. at 21–22 (1971) (holding that wearing a "Fuck the Draft" jacket in public did not violate the privacy of bystanders to a sufficiently intolerable extent to justify prosecution).

33. *See* Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 984 (2003).

34. *See, e.g.*, ROSEN, *supra* note 18, at 17 ("Many of the liberties on this remarkable list are better conceived as invasions of privacy than as gender discrimination.").

"some retreat from the world," and that invasion of privacy causes the individual "mental pain and distress."[35] They also noted that some breaches of privacy can "destroy[] at once robustness of thought and delicacy of feeling."[36] That injury can be defined as harm to the individual's autonomy.[37] The harms to privacy are not to reputation like defamation, nor are they to economic interests like a breach of contract. Rather, the harms are psychic in nature, such as "incivility, lack of respect, or causing emotional angst."[38] Another category of injury related to privacy includes privacy architecture that involves "the creation of the risk that a person might be harmed in the future."[39]

B. PRIVACY IN THE DIGITAL AGE

Rapid technological advancement has made retreat from the world a more complicated concept. Moore's Law states that the number of transistors that can fit on a microchip doubles every two years.[40] At the time of Prosser's article, engineers were putting around thirty transistors on a chip.[41] In 2012, Intel expects to release its latest chip, "Poulson," which it claims will hold 3.1 billion transistors.[42] This exponential growth in the memory and speed of processors has made possible technological advancement as well as new ways to encroach on privacy.[43] The Internet, computers, cameras, and other technologies have collected and exposed individuals' personal information in ways unforeseen by Prosser and earlier privacy scholars.[44]

---

35. Warren & Brandeis, *supra* note 9, at 196.

36. *Id.*

37. Autonomy harms are "privacy harms affect the nature of society and impede individual activities that contribute to the greater social good." Solove, *Taxonomy*, *supra* note 13, at 488.

38. *Id.* at 486.

39. *Id.* at 487.

40. *Excerpts from A Conversation with Gordon Moore: Moore's Law*, INTEL.COM (2005), *available at* ftp://download.intel.com/museum/ Moores_ Law/Video-Transcripts/Excepts_A_Conversation_with_Gordon_ Moore.pdf.

41. *Id.*

42. Pauline Nist, *Itanium Poulson Update - Greater Parallelism, New Instruction Replay & More: Catch the Details from Hotchips!*, THE SERVER ROOM BLOG (Aug. 19, 2011), http://communities.intel.com/community/openportit/ server/blog/2011/08/19/itanium-poulson-update--greater-parallelism-new-in struction-replay-more-catch-the-details-from-hotchips.

43. *See* SOLOVE, DIGITAL PERSON, *supra* note 6, at 14 ("As processing speeds accelerated and as memory ballooned, computers provided a vastly increased ability to collect, search, analyze, and transfer records.")

44. Solove, *Taxonomy*, *supra* note 13, at 478 ("[N]ew technologies have

1. Privacy-breaching Technology

To demonstrate the new threats to privacy, students at Fordham Law School compiled a fifteen-page personal dossier on Justice Antonin Scalia based on information found on the Web.[45] Such a dossier goes well beyond the newspaper accounts of Samuel Warren's daughter's wedding that inspired "The Right to Privacy."[46] The threats to privacy contemplated by Warren and Brandeis and Prosser do not map neatly onto twenty-first century technology.[47] Cameras, cell-phones, consumer transactions, Global Positioning System (GPS) devices in cars, tollbooths, email, monitoring software, cookies, and other technologies produce vast amounts of personal data in increasingly large and powerful databases.[48] Consumers' quotidian transactions that once left no trace now leave behind a digital trail.[49] The Internet has created new activities that leave behind their own traceable digital trails.[50] Technology allows consumers to shop from the privacy of their homes, but online shopping produces data that can be cataloged, so even though any single transaction might be noticed by fewer onlookers, the details of that transaction will be remembered in the consumer's "digital dossier."[51]

---

given rise to a panoply of new privacy harms.").

45. *See* Noam Cohen, *Law Students Teach Scalia About Privacy and the Web*, N.Y. TIMES, May 18, 2009, at B3. Justice Scalia called the exercise "an example of perfectly legal, abominably poor judgment." *Id.*

46. ROSEN, *supra* note 18, at 7 ("What outraged Brandeis and Warren was a mild society item in the Boston *Saturday Evening Gazette* that described a lavish breakfast party Warren himself had put on for his daughter's wedding.").

47. *See generally* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) (analyzing privacy issues with modern technology).

48. *See, e.g.*, ROBERT O'HARROW, JR., NO PLACE TO HIDE 283–300 (2005); Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1473–1501 (2000).

49. *See* O'HARROW, *supra* note 48, at 284–85 (describing the types of data companies record: web-browsing data, TiVO data, credit card transactions, etc.).

50. "Clickstream data," for example, includes "data about [the user's] ISP, computer hardware and software, the website she linked from, and exactly what parts of the website she explored and for how long." SOLOVE, DIGITAL PERSON, *supra* note 6, at 23–24.

51. *Id.* at 1 ("A dossier is a collection of detailed data about an individual.").

2. Threats to Privacy from Aggregation

Although individuals might not expect any particular personal datum to remain secret, aggregation of personal data "reveals facts about data subjects in ways far beyond anything they expected when they gave out the data."[52] Transactional data can be analyzed in the aggregate to identify market trends or it can be linked to individuals to identify individual habits.[53] Aggregation was historically not considered among privacy harms because the technology making aggregation possible and profitable came about in recent decades.[54] In at least one case, the Supreme Court recognized aggregation of public information as an intrusion into privacy, noting "the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole."[55] Justice Sotomayor, concurring in *United States v. Jones*, discussed the dangers to privacy in the digital age when the government aggregates personal data, proposing that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[56] Aggregation violates privacy by revealing aspects of a person's private life he might prefer to be kept private.[57] But aggregation cre-

---

52. Solove, *Taxonomy*, *supra* note 13, at 507. "When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected." *Id.* at 506.

53. *See id.* at 511–12.

54. *Id.* at 505–06 (describing the apprehension that arose in the 1960s when the rise of computers allowed for aggregation of data).

55. U.S. Dep't. of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 764 (1989) (holding disclosure of Federal Bureau of Investigation rap sheets to be an unwarranted invasion of personal privacy). Other courts, however, have found this analysis of aggregation inapplicable outside Freedom of Information Act cases. Solove, *Taxonomy*, *supra* note 13, at 519.

56. United States v. Jones, 565 U.S. No. 10–1259, 5 (2012) (Sotomayor, J., concurring). The government argued warrantless GPS tracking is permissible because individuals have no expectation of privacy in public spaces, but Respondent argued the expectation to be seen at discrete times and places is not the expectation for each discrete sighting to be aggregated. *See* Brief of Electronic Privacy Information Center (EPIC) et al. as Amici Curiae Supporting Respondent, United States v. Jones, No. 10-1259, 2011 WL 4564007 (Oct. 3, 2011) ("GPS tracking systems allow officers to comb stored data to conduct new searches using a suspect's historical location data, as well as to aggregate data from a variety of sources, both public and private.").

57. Solove, *Taxonomy*, *supra* note 13, at 507 (aggregation upsets individuals' expectations about "certain limits on what is known about them and on what others will find out").

ates distorted summaries of individuals because "the data is often reductive and disconnected from the original context in which it was gathered."[58] The harm from data-mining generally comes from "being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge."[59]

3. Existing Data Privacy Laws

Congress has enacted a variety of laws intended to protect privacy in specific, limited contexts. The Privacy Act of 1974 governs governmental agencies' collection and maintenance of personal information.[60] The Cable Communications Policy Act of 1984 "requires cable operators to inform subscribers about the nature and uses of personal information collected"[61] and to obtain consent from subscribers before collecting personal information. Additionaly it prohibits cable operators from disclosing personal information unless doing so is necessary for "legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber."[62] The Electronic Communications Privacy Act of 1986 "restricts the interception of transmitted communications and the searching of stored communications."[63] The Computer Matching and Privacy Protection Act of 1988 restricts disclosure of information between federal agencies and requires agencies to provide individuals with a copy of their records on request.[64] The Driver's Privacy Protection Act of 1994 deals with the issue of the government selling data to private parties by restricting the disclosure and resale of information obtained by state departments of motor vehicles.[65] The Gramm-Leach-Bliley Act of 1999 prohibits financial institutions from sharing nonpublic personal information with third parties without allowing consumers to

58. *Id.* at 507.
59. ROSEN, *supra* note 18, at 8.
60. 5 U.S.C. § 552(a) (2006).
61. SOLOVE, DIGITAL PERSON, *supra* note 6, at 68.
62. 47 U.S.C. § 551(c)(2)(A) (2006).
63. 18 U.S.C. §§ 2510–22; 2701–10 (2006). *See* SOLOVE, DIGITAL PERSON, *supra* note 6, at 68.
64. 5 U.S.C. § 552(a) (2006).
65. 18 U.S.C. § 2721 (2006). *See* SOLOVE, DIGITAL PERSON, *supra* note 6, at 69.

opt out.[66] States too have statutes protecting data privacy, such as the Minnesota Data Practices Act, which governs the "collection, creation, storage, maintenance, dissemination, and access to government data in government entities."[67] All these statutes contain loopholes that allow for privacy to be breached.[68] The Federal Trade Commission (FTC) has recommended a set of voluntary data privacy principles for private entities to adopt.[69] The four principles are: 1) giving consumers "transparency and control"; 2) "reasonable security and limited data retention"; 3) notice of privacy policy changes; and 4) "affirmative express consent before they use sensitive data."[70] The FTC does not mandate adoption of these principles, but some entities have voluntarily incorporated them into their privacy policies.[71] More recently, the White House released its Consumer Privacy Bill of Rights and called on Congress to codify its contents and grant the FTC authority to enforce it.[72]

4. Redefining the Right to Privacy in the Digital Age

The broadening universe of data sources has led to new ways of conceptualizing the right to privacy. A brief overview of these approaches provides a useful toolbox for evaluat-

---

66. 15 U.S.C. § 6802 (2006); *see* SOLOVE, DIGITAL PERSON, *supra* note 6, at 70.

67. MINN. STAT. § 13.01 subd. 3 (2011). The statute also limits the state's use of cookies to collect information. MINN. STAT. § 13.15 (2011).

68. The Privacy Act of 1974, Computer Matching and Privacy Protection Act, and Minnesota Data Practices Act govern only government records. 5 U.S.C. § 552(a) (2006); MINN. STAT. § 13.01 subd. 3 (2011). The Cable Communications Policy Act of 1984 allows disclosure of personal information as part of "legitimate business activity." 47 U.S.C. § 551(c)(2)(A) (2006). The Electronic Communications Privacy Act "is not well-tailored to addressing a large portion of private-sector information gathering in cyberspace." SOLOVE, DIGITAL PERSON, *supra* note 6, at 69. The Driver's Privacy Protection Act applies only to departments of motor vehicles and not to other state agencies. *Id.* Gramm-Leach-Bliley's "opt-out default creates incentives for privacy notices that lead to inaction by the consumer." Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1241 (2002).

69. FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 11–12 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter FTC STAFF REPORT].

70. *Id.*

71. *Id.*

72. WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 35–36 (2012).

ing twenty-first century privacy breaches. Daniel Solove's *Taxonomy of Privacy* attempts to flesh out the right to privacy by naming four categories of harmful activities having to do with personal information: 1) collection, 2) processing, 3) dissemination, and 4) invasion.[73]

Neil Richards suggests moving away from the concept of privacy in the realm of personal data and instead conceptualizing the problem in terms of data protection and confidentiality.[74] Richards argues that "'data protection' can draw attention to the specific problems associated with databases without risking an association with all of the assorted baggage that privacy connotes."[75] Based on the data protection paradigm, the 1996 European Community Directive on Data Protection supplies a Digital Age framework for personal data.[76] The Directive limits acceptable uses of personal data and allows individuals to maintain some control over their personal information.[77] It also requires member countries to balance privacy rights with the free flow of data.[78] The five principles of the EU Directive are that personal data are: 1) "processed fairly and lawfully"; 2) "collected for specified, explicit and legitimate purposes"; 3) "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"; 4) "accurate"; and 5) "kept in a form which permits identification of data subjects for no longer than is necessary."[79] This approach is consistent with Westin's definition of privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is

---

73. Solove, *Taxonomy*, *supra* note 13, at 489. This Note will focus on harms from processing and dissemination, because these categories tend to include the harms associated with political data-mining.

74. Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1135 (2006).

75. *Id.* at 1137; *see also* Raymond T. Nimmer, *"Privacy" and "Data Protection" Defined-—"Data Protection" as a Contrasting Idea*, *in* THE LAW OF COMPUTER TECHNOLOGY 17:5 (4th ed. 2011) (noting that data protection "centers on control of personally identifiable data, rather than on protected secrecy.").

76. Council Directive 95/46, art. 1, 1995 O.J. (L 281) 31, 38 (EC) [hereinafter EU DIRECTIVE].

77. *Id.*

78. *Id.* at art. 1 ("Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.").

79. *Id.* at art. 6.

communicated to others."[80]

Another useful approach to privacy in the computing age may be "contextual integrity."[81] Individuals pass through a variety of different spheres or contexts in their day-to-day lives, and each sphere comes with its own set of norms.[82] Personal information that may be shared in certain contexts cannot be appropriately shared in others.[83] Privacy is breached when these norms are transgressed.[84] For example, a vendor who maintains records of its customers' purchases and contact information operates within these norms, but the vendor transgresses norms of appropriateness and distribution by sharing customer information with third parties.[85] Cheaper, more powerful technology lowers the cost of breaching contextual integrity by recording personal information and storing it for a fraction of what it would cost to manually do so. Furthermore, aggregating data adds value, thus making the practice of systematically breaching contextual integrity profitable.

C. DATA-MINING CONSUMER INFORMATION

The parties to a financial transaction are said to equally own the facts to the transaction.[86] But advancing technology has made collection, aggregation, and dissemination of personal information feasible and profitable for an increasing number of actors, many of whom are not present at the initial transaction.[87] The data from these transactions are compiled in con-

---

80. WESTIN, *supra* note 23, at 7.

81. Nissenbaum, *supra* note 47, at 136–43 (describing the informational norms of "appropriateness" and "distribution" and arguing that privacy is breached when these norms are transgressed).

82. Individuals "are at home with families, they go to work, they seek medical care, visit friends, consult with psychiatrists, talk with lawyers, go to the bank, attend religious services, vote, shop," and norms in each context govern "roles, expectations, actions, and practices." *Id.* at 137.

83. "[T]he patient shares information about his or her physical condition with the physician but not vice versa." *Id.* at 138. "[W]e are not (at least in the United States) expected to share our religious affiliation with employers, financial standing with friends and acquaintances, performance at work with physicians, etc." *Id.* at 138–39.

84. *Id.* at 138 ("[A] complaint that privacy has been violated is sound in the event that one or the other types of the informational norms has been transgressed.").

85. *Id.* at 152–53.

86. Froomkin, *supra* note 48, at 1502.

87. *See* SOLOVE, DIGITAL PERSON, *supra* note 6, at 3–4 (2004) ("Countless companies maintain computerized records of their customers' preferences,

sumer databases, aggregated, and sold.[88] While this sort of consumer data-mining has existed for years, increasingly powerful online tools now track users' movements around the web and compile digital dossiers.[89] The commodification of personal data allows websites to provide users with content free of charge; users pay for content with their personal data instead of money.[90] Shopper loyalty cards, another major source of consumer data, make discounts and coupons available to users.[91] Most consumers probably understand that vendors compile data about their customers, and many consumers probably understand that they trade their personal information in exchange for the free use of websites, but "[f]ewer are aware that this information is shipped off and aggregated in data warehouses where it is organized, stored, and analyzed."[92]

1. Methods of Collecting Consumer Data

"Big Data" is a multi-billion dollar industry.[93] Firms amass data on everything from soil quality to medical information and

---

purchase, and activities. . . . [a]nd there are hundreds of companies people aren't even aware of that maintain their personal information."); *see also* EU DIRECTIVE, *supra* note 76, at paragraph (4) ("[T]he progress made in information technology is making the processing and exchange of such data considerably easier.").

88. *See* SOLOVE, DIGITAL PERSON, *supra* note 6, at 18–21. "There are around five database compilers that have data on almost all households in the United States." *Id.* at 20.

89. *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010, at W1. "Tracking isn't new. But the technology is growing so powerful and ubiquitous that even some of America's biggest sites say they were unaware, until informed by the Journal, that they were installing intrusive files on visitors' computers." *Id.*

90. *See generally* FTC STAFF REPORT, *supra* note 69, at i ("[P]otential benefits of the practice to consumers, include[] the free online content that online advertising generally supports, the personalized advertising that many consumers may value, and a potential reduction in unwanted advertising.").

91. *See, e.g.*, Dan Sewell, *Kroger Really Knows About Its Customers' Buying Habits*, THE LEDGER, (Jan. 6, 2009), http://www.theledger.com /article/20090106/NEWS/901060335. These cards have also been used to alert consumers to product recalls. Steve Raabe, *Shopper-card Data Traced for Other Uses*, DENV. POST (June 10, 2010), http://www.denverpost.com/business /ci_15264783.

92. Nissenbaum, *supra* note 47, at 121.

93. *See* Quentin Hardy, *The Big Business of 'Big Data'*, NYTIMES.COM (Oct. 24, 2011) http://bits.blogs.nytimes.com/2011/10/24/big-data/ ?scp=1&sq=data%20mining&st=cse (noting that Hewlett-Packard recently bought a data company named Autonomy for $10.3 billion).

"cleverly sift[] through it to find and exploit new patterns and relationships."[94] The value from this activity comes from being able to target ads for goods and services to likely customers, thus limiting the waste of dollars spent on advertising to non-customers.[95] When an individual gives out personal information, he typically does so not expecting that data to be sold to third parties for uses unrelated to the original transaction.[96] Users of frequent shopper cards trade their contact information for coupons and discounts.[97] Vendors, such as grocery stores, track customers' purchases through the shopper cards, allowing them to target relevant coupons at particular customers.[98] But third party data-miners may purchase shopper card data, aggregate it with other personal data, and resell it to other vendors without the individual's knowledge.

A variety of data-mining tools surreptitiously gather information from web users. For many years, "cookies" have recorded the websites people visit.[99] New tools "scan in real time what people are doing on a Web page, then instantly assess location, income, shopping interests and even medical conditions."[100] The user need not complete a transaction for a tracker to obtain information; a mere web search provides useful data.[101] The information gathered by these tools is bought and

---

94. *Id.* Hardy makes the case that the Big Data bubble may be about to burst as lofty expectations fall in line with reality and the technology "turn[s] from a competitive edge into a must-have." *Id.*

95. *Id.* ("When you know what someone has purchased, you can make a case of what ad to put in front of them next.").

96. "Secondary use resembles breach of confidentiality, in that there is a betrayal of the person's expectations when giving out information." Solove, *Taxonomy*, *supra* note 13, at 522.

97. Sewell, *supra* note 91.

98. *Id.* Simon Hay, CEO of Kroger's data-mining firm, dunnhumby, notes the dangers to Kroger of selling customer information to third parties: "We understand that this is long-term, and if we do anything to exploit that relationship, then we destroy the value for our clients." *Id.*

99. Angwin, *supra* note 89, at W1.

100. *Id.* "Tracking is done by tiny files and programs known as 'cookies,' 'Flash cookies' and 'beacons.'" *Id.*

101. The FTC provides the following example:

> [A] consumer visits a travel website and searches for airline flights to New York City. The consumer does not purchase any tickets, but later visits the website of a local newspaper to read about the Washington Nationals baseball team. While on the newspaper's website, the consumer receives an advertisement from an airline featuring flights from Washington D.C. to New York City.

FTC STAFF REPORT *supra* note 69, at 3.

sold amongst a network of data firms and advertisers for the purpose of creating precisely targeted ads to appeal to particular users.[102] Some firms analyze the data to predict the user's tastes and preferences.[103] Users themselves likely realize how many tools are tracking them at any given time, but, more surprisingly, many website proprietors know how many cookies, beacons, and other tools their own sites are installing on users' computers.[104]

2. Harms from Consumer Data-Mining

In a situation where a citizen's consumer, Internet, and political transactions are recorded, compiled, and sold, the citizen suffers at least two injuries. First, knowing that his transactions are being observed—let alone recorded, compiled, and commoditized—may cause the citizen to alter his behavior.[105] In this way, the citizen's autonomy is harmed; he may be discouraged from consumption or political participation that he believes will be made public.[106] Second, the aggregation of consumer and political transaction data creates digital dossiers—rich descriptions of citizens' lives that go beyond what an individual consents to as part of his public persona.[107] Both harms violate the individual's autonomy by creating an imbalance in

---

102. *See generally* Angwin, *supra* note 89, at W1. *See also* FTC STAFF REPORT, *supra* note 69, at i (defining online behavioral advertising as "the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests.").

103. Angwin, *supra* note 89, at W2. "[S]ome tracking companies use probability algorithms to try to pair what they know about a person's online behavior with data from offline sources about household income, geography and education, among other things." *Id.*

104. *Id.* The article reports that Comcast was unaware that Comcast.net installed fifty-five cookies on the Wall Street Journal's test computer. One tracking company, BlueKai, allows individuals to see their digital profile and opt out of tracking. BlueKai Registry, BLUEKAI, http://www.bluekai.com/registry/ (last visited Feb. 27, 2012). The Wall Street Journal recently updated its privacy policy to "allow the site to connect personally identifiable information with Web browsing data without user consent." Joe Coscarelli, *The Wall Street Journal's New Privacy Policy Is Everything They Taught Us to Fear*, DAILY INTEL, (Sept. 28, 2011), http://nymag.com/daily/intel/2011/09/the_wall_street_journals_new_p.html.

105. Solove, *Taxonomy*, *supra* note 13, at 488 (surveillance can have a chilling effect on individuals, "making them less likely to attend political rallies or criticize popular views.").

106. *Id.*

107. SOLOVE, DIGITAL PERSON, *supra* note 6, at 1.

power relationships surrounding individual decision-making.[108] Injuries to individual autonomy in the political sphere may be uniquely harmful and require unique remedies.[109]

II. POLITICAL DATA-MINING

If the problem with data-mining in general is that it "seek[s] to shape and predict individual behavior according to externally-determined trajectories of opportunity and desire,"[110] we should be particularly wary of its role in electoral politics. Aristotle's John Phillips admits, "[e]very campaign that we work with wants you to believe that it's shoe leather that wins the race, or great issues, or the love of the people, but the fact of the matter is a lot of it is the nitty-gritty organization."[111] Data-mining in the consumer sphere spurs concerns over consumer privacy, but when the same techniques are used in the political sphere "it begins to pull back the curtain of one of the most protected locations in America, the voting booth."[112] In the past three decades, political candidates have increasingly come to rely on extensive, detailed voter databases—such as Voter Vault, Catalist, and Aristotle—compiled from both publicly available election data and the consumer data compiled over the years by businesses.[113] Catalist, a privately-owned progressive database, includes "data from frequent-buyer cards at supermarkets and pharmacies, hunting- and fishing-license registries, catalog- and magazine-subscription lists, membership rolls from unions, professional associations, and advocacy groups such as the ACLU and the NRA."[114] In 2004, the Repub-

---

108. Richards, *supra* note 74, at 1094.

109. The secret ballot, after all, affords a zone of privacy for the voter that consumers are not entitled to. Ari Schwartz, an analyst at the Center for Democracy and Technology said "we are especially concerned when we are talking about voting and citizenship, things that are so central to the election process." Wayne, *supra* note 7, at A10.

110. Cohen, *Examined Lives*, *supra* note 8, at 1376.

111. Verini, *supra* note 5.

112. Wayne, *supra* note 7, at A10.

113. *See* Verini, *supra* note 5 ("Aristotle can tell its clients more than just the predictable stuff—where you live, your phone number, who lives with you, your birthday, how many children you have. It may also know how much you make, how much your house is worth, what kind of car you drive, what Web sites you visit, and whether you went to college, attend church, own guns, have had a sex change, or have been convicted of a felony or sex crime. It can pry into every corner of your life."). Every President since Ronald Reagan has hired Aristotle as a consultant. *Id.*

114. Graff, *supra* note 5, at 40.

lican National Committee (RNC) used its database, Voter Vault, to establish data dominance by micro-targeting voters who might otherwise have been excluded from mail drops.[115] By 2008, the Democrats had surpassed the RNC's data capabilities through the privately run Catalist, and now the parties are engaged in a data-arms race for 2012.[116] Matching personal data to specific individuals allows candidates to send direct mail to voters, canvas potentially friendly voters living in unfriendly territory, and prospect potential donors.[117] It also allows campaigns to evaluate likely voters based on patterns in data and surveys, and then predict likely voting habits.[118]

While consumer data is compiled, aggregated, and sold by private firms, an increasing amount of data on citizens is made publicly available through government websites. Of particular interest to political data-miners is data on voters and campaign finance.[119] Voter registration information is available through many states' Secretary of State[120] as well as through private services.[121] Campaign finance data at the state, federal, and local levels are even easier to access online.[122] With relatively lit-

---

115. *See id*.

116. Kate Kaye, *Republican Party Aims to Match Democrats' Data Strength*, CLICKZ (June 6, 2011), http://www.clickz.com/clickz/news/2076532/republican-party-aims-match-democrats-strength; Sifry, *supra* note 4.

117. *See, e.g.*, Wayne, *supra* note 7, at A10 (describing how the political consulting firm Aristotle provides data that allows candidates to send personalized letters to specific types of donors and to target "Fat Cats" for fundraising).

118. Graff, *supra* note 5, at 40 ("[S]ome of the strongest predictors of political ideology are things like education, homeownership, income level, and household size. Religion and gun ownership are the two most powerful predictors of partisan ID.").

119. Past voting and donation history are some of the most accurate predictors of future voting and donation habits.

120. *See, e.g.*, *Confidentiality Notice*, OFFICE OF THE MINNESOTA SECRETARY OF STATE, http://www.sos.state.mn.us/index.aspx?page=207 (last visited Mar. 9, 2012) ("Access to the data that you supply on your voter registration application is restricted to elections officials and to those who obtain the list for political, law enforcement and jury selection purposes.").

121. *See, e.g.*, VOTER HISTORY, http://voterhistory.com/ (last visited Mar. 9, 2012) ("For each voter, we have 10 year voting history (that's 5 cycles for general, primary and joint(city) elections); demographic (data); home appraised value; and (future) personality trait data that can be meaningful to targeting.").

122. *See Campaign Finance Reports Search and Lists*, TEXAS ETHICS COMMISSION, http://www.ethics.state.tx.us/dfs/search_CF.htm (last visited Mar. 9, 2012). For example, the Texas Ethics Commission allows anyone visit-

tle effort and cost, a data-miner can compile a useful voter database from just publicly available data.[123] A data-miner can then purchase consumer data and match it to the voting and contribution data based on names and contact information.[124] The result is a database that can quickly identify a citizen's name, address, employer, occupation, phone number, email address, party affiliation, voting history, donor history, purchasing habits, and web browsing history.[125]

Campaigns running their own databases from just publicly available sources can augment their data with information gleaned from their own voter contact, through canvassing, phone banking, or fund-raising. The most sophisticated private database operators allow campaigns that buy their lists to add data to the master database from their own campaign databases and voter contact.[126] When a campaign gathers information for its own use, the voter at least knows who is using the data, but when voter data is compiled across candidates and election cycles in large national databases, the voter can lose sight of his information.

Campaigns have long used voter registration and history data to target likely voters.[127] Contribution history is an accurate predictor of future contributions, so this data has been a staple of political fundraising. Federal contribution data is readily available, but the Federal Election Campaign Act prohibits use of this data for fundraising or commercial purposes.[128] Aggregation of personal data from a variety of sources gives campaigns the power to create more detailed profiles of

---

ing its website to download its entire campaign finance report database, including names, addresses, occupations, employers, and contribution histories of donors to political campaigns in Texas. *Id.*

123. *See id.*

124. *See, e.g.*, Wayne, *supra* note 7, at A10 (noting that Aristotle blends voter data it has collected with consumer data purchased from other databases).

125. *Id.*

126. Catalist asks its clients to report data they find during the campaign, either in real-time or at the end of the campaign. Graff, *supra* note 5, at 43.

127. Verini, *supra* note 5 (recounting the data operations of Presidents Carter, Kennedy, and Lincoln).

128. 2 U.S.C. § 438(a)(4) (2006) ("[A]ny information copied from such reports or statements may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes, other than using the name and address of any political committee to solicit contributions from such committee.").

individual voters than ever before.[129] One important use of these profiles has been micro-targeting, whereby a campaign can tailor its message to certain voters with relative precision.[130] Where in the past a campaign might send a piece of direct mail to every female who voted in three of the past four Democratic primaries, now campaigns can target, say, Volvo drivers, or visitors to The Drudge Report. Campaigns can micro-target to encourage friendly voters to cast ballots for a candidate, or they can micro-target to suppress their opponent's voters.[131] By some estimates, micro-targeting allowed George W. Bush to win Ohio, and thus reelection, in 2004.[132]

New methods of politicking yield more data. President Obama's campaign Facebook page has twenty-three million "likes" and an app to gather data on all those twenty-three million users.[133] President Obama's campaign shares data from field-level organizers up the hierarchy through its own social networking tool.[134] The ability of databases to keep track of

---

129. Graff, *supra* note 5, at 39 ("In past years, campaigns couldn't sort the electorate and use finely grained outreach and mobilization techniques. Today, thanks to expensive and powerful databases like the GOP's Voter Vault and the progressive startup Catalist, targeting voting blocs is as simple as checking boxes on a computer screen.").

130. In 2008, the Obama campaign was able to "custom-tailor cable-television ads down to the Zip Code in Iowa, or send a canvasser to a voter's doorstep armed with a computer-generated picture of that person's political personality." Verini, *supra* note 5.

131. *See* Nichole Rustin-Paschal, Symposium, *Online Behavioral Advertising and Deceptive Campaign Tactics: Policy Issues*, 19 WM & MARY BILL RTS. J. 907, 913 (2011) ("In an increasingly information-based society, deceptive campaigns will likely be launched in ways that take advantage of tools provided by web-based technologies for communicating and organizing.").

132. Vanity Fair reports that in 2004 Karl Rove took advantage of micro-targeting to "sen[d] shock troops into Democratic pockets of blue-collar workers and minorities with personalized appeals to the churchgoing, the gun-owning, the abortion-hating. The result was a lead of 130,000 votes that tipped the election to Bush." Verini, *supra* note 5. On the other hand, Democratic National Committee chairman Terry McAuliffe remarked, upon learning his party's database contained 1.1 million incorrect entries in Florida in 2000, "Don't you think we could have found 537 votes if we had corrected that information earlier and contacted 1.1 million more people?" Graff, *supra* note 5, at 40.

133. Sifry, *supra* note 4 ("Users of the Obama 2012 - Are You In? app are not only giving the campaign personal data like their name, gender, birthday, current city, religion and political views, they are sharing their list of friends and information those friends share, like their birthday, current city, religion and political views.").

134. *Id.* (NationalField allows the campaign to compile "information they

voters who move across state lines eliminates the old problem of losing data on voters who move.[135] Local campaigns also take advantage of big voter databases; Fort Wayne, Indiana Republican mayoral candidate Paula Hughes used Voter Vault in her unsuccessful 2011 campaign.[136] Although Hughes lost, the data collected by her campaign will be valuable for candidates in the 2012 cycle.[137] At the cutting edge of political data-mining, the Obama campaign's "Dreamcatcher" project will use text analytics to glean political beliefs and motivations from voters' narratives entered on the campaign's website.[138]

Political data-mining raises a variety of concerns that this Note will only briefly discuss. Databases containing personal voter information have been compromised in the past. One of the largest voter databases, Aristotle, was caught selling data to unverified individuals, such as "Britney Spears" and "Condoleezza Rice," in 2003.[139] Aristotle also falsely claimed at the time that it "never added information from market research to its voter files"[140] Aristotle sells data to Democrats and Republicans, as well as candidates from Ukraine, Algeria, Kosovo, Venezuela, and the Palestinian Fatah party.[141] The Obama and McCain campaigns' computers were hacked during the 2008 election.[142] Micro-targeting can lead to a different set of harms,

---

are gathering as they work on tasks like signing up volunteers, knocking on doors, identifying likely voters and dealing with problems," as well as "qualitative data.").

135. Graff, *supra* note 5, at 43.

136. Tom LoBianco, *Ind. Dems, GOP Use Mayoral Races to Build for 2012*, POST TRIBUNE (Indiana) (Oct. 30, 2011), http://posttrib.suntimes.com/news/8512679-418/ind-dems-gop-use-mayoral-races-to-build-for-2012.html ("Hughes has gotten access to more voters and the state party has updated its vast store of information relying on phone calls and canvassing done on Hughes' behalf.").

137. *See id.*

138. Sasha Issenberg, *Project Dreamcatcher: How cutting-edge text analytics can help the Obama campaign determine voters' hopes and fears*, SLATE.COM (Jan. 13, 2012), http://www.slate.com/articles/news_and_politics/victory_lab/2012/01/project_dreamcatcher_how_cutting_edge_text_analytics_can_help_the_obama_campaign_determine_voters_hopes_and_fears_.html.

139. Kim Zetter, *For Sale: The American Voter*, WIRED.COM (Dec. 11, 2003), http://www.wired.com/politics/security/news/2003/12/61543.

140. *Id.* Aristotle now acknowledges "that it adds consumer marketing data to voter information." Kim Zetter, *Voter Privacy Is Gone–Get Over It*, WIRED.COM (Jan. 31, 2008), http://www.wired.com/threatlevel/2008/01/voter-privacy-i/.

141. Verini, *supra* note 5.

142. Philip N. Howard & Daniel Kreiss, *Political Parties and Voter Privacy:*

especially voter deception.[143]

III. APPROACHES TO PROTECTING VOTER PRIVACY

If enacted, the Consumer Privacy Bill of Rights will change the ways private firms collect consumer data and at least have some effect on the voter data campaigns gather from data-miners, but it is not clear whether the codified Bill would apply directly to political data-mining.[144] The Bill's principles should apply to political data-mining, so a voter privacy measure would be a valuable outcome of the multi-stakeholder process encouraged by the White House.[145] American democracy already recognizes and protects voter privacy, at least at the polling place.[146] But political life encompasses more than merely casting a ballot; new technology allows for broad dissemination of views and new means of debate.[147] Political participation online may be stifled without privacy protections—scrutiny of online voter activity may distort voter participation.[148] Given

---

Australia, Canada,the United Kingdom, and United States in Comparative Perspective, FIRST MONDAY (2010), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2975/2627.

143. *See* Rustin-Paschal, *supra* note 131, at 914 (arguing that the Internet "serve[s] not only to bring people together, but to launch deceptive campaigns"); Daniel Kreiss, *Yes We Can (Profile You)*, 64 STAN. L. REV. ONLINE 70, 74 (2012), *available at* http://www.stanfordlawreview.org/online/privacy-paradox/political-data. (noting that micro-targeting means "campaigns can develop narrow appeals based on ideology and self-interest and direct them to different groups of voters, appearing to be all things to all people.").

144. *See* WHITE HOUSE, *supra* note 72, at 10 ("The Consumer Privacy Bill of Rights applies to commercial uses of personal data.").

145. *See id.* at 23–24 (discussing the multi-stakeholder process).

146. *See* Nissenbaum, *supra* note 47, at 146 ("From the moment [voters] cross the threshold, information flows are highly regulated, from what elections officers can ask them to what they can ask officers, what voters are required to document in writing, who sees it, what happens to the vote cast and who sees that, what exit pollsters can ask citizens as they leave—for whom they voted but not voters' names—and what the exit pollsters are free to disseminate publicly.").

147. *See* Gardner, *supra* note 1, at 928 ("But political participation in modern democratic life can take many forms: financial contributions to candidates, political parties, and advocacy groups; petition signing; political speech and debate; communication with and lobbying of officials; attending public meetings; holding office . . . paying taxes, obeying the law, or performing public service or charitable work in one's community.").

148. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1651 (1999) ("[W]ho will speak or listen when this behavior leaves

that accessing democratic forums on the Internet creates a traceable digital trail, "merely listening on the Internet becomes a speech-act."[149] In this way, data-mining of political information can compromise self-government while falling under First Amendment protection. Political data-mining can also detract from voter autonomy when "[i]ts perfected surveillance of naked thought's digital expression short-circuits the individual's own process of decisionmaking."[150]

A. PAST ATTEMPTS TO PROTECT VOTER PRIVACY

If privacy is defined as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others,"[151] then existing law fails to protect the privacy of individuals from political data-mining. Citizens lose sight of bits of data gleaned from consumer transactions, campaign contributions, and government documents once that data comes into the possession of other parties to a transaction.[152] Citizens have limited control at best over what third parties gain access to their information.[153] Aggregation of data from various sources provides data-miners with a fuller picture of an individual than they intend to reveal.[154] When an individual buys a car, he does not expect that transaction to lead to a political consultant categorizing him as a particular type of voter likely to be susceptible to a certain political ad.[155]

1. Existing Law Does Not Protect Data Privacy

The four privacy torts appear inadequate to deal with technology-driven threats to privacy. Intrusion upon seclusion protects material of a particularly sensitive nature, not the

---

finely-grained data trails in a fashion that is difficult to understand or anticipate?").

149. *Id.* at 1652.

150. *Id.* at 1656.

151. WESTIN, *supra* note 21, at 7.

152. *See* Solove, *Taxonomy*, *supra* note 13, at 506–07.

153. *See id.*

154. *See* Solove, *Taxonomy*, *supra* note 13, at 507 ("Aggregation upsets these expectations, because it involves the combination of data in new, potentially unanticipated ways to reveal facts about a person that are not readily known.").

155. *See, e.g.*, Graff, *supra* note 5, at 41 ("Jaguar, Land Rover, and Porsche owners tend to be more Republican, while Subaru, Hyundai, and Volvo drivers lean Democratic.").

seemingly mundane and often public details of consumer transactions.[156] Public disclosure of private facts also protects only information that would be "highly offensive," and the sale of data between private databases does not rise to a sufficient level of publicity.[157] False light publicity protects only against reputational harms, not the injuries to autonomy inflicted by data-mining.[158] Appropriation of name or likeness protects the value of an individual's identity, not the value added from aggregation.[159] Statutes intended to protect privacy seem similarly ill equipped to handle high-tech threats to privacy.[160]

The approach to protecting voter privacy in the United States has been piecemeal and, many would argue, unsuccessful. Two substantial problems stand in the way of voter privacy legislation: voter apathy and the First Amendment.[161] Most data compilation occurs by a gradual process of accretion from transactions, so the violation of privacy goes unnoticed to the individual.[162] Consequently, most individuals do not know the extent to which they are being profiled. Laws that burden political speech must serve a compelling governmental interest and be narrowly tailored to serve that interest.[163] How restrictive a regime can be applied to political data-mining thus depends in part on whether the activity of data-miners is speech at all and, if so, whether it is commercial speech (which receives limited First Amendment protection)[164] or political speech (which re-

---

156. SOLOVE, DIGITAL PERSON, *supra* note 6, at 59 ("[C]ourts have rejected intrusion actions based on obtaining a person's unlisted phone number, selling the names of magazine subscribers . . . and collecting and disclosing an individual's past insurance history.").

157. *Id.* at 59–60.

158. *Id.* at 60.

159. *Id.* at 60–61.

160. *See supra* note 68.

161. *See, e.g.*, Howard & Kreiss, *supra* note 142 ("On First Amendment grounds, provided they remain non–state actors candidates and parties enjoy broad latitude with respect to their data practices."); Bartnicki v. Vopper, 532 U.S. 514, 534 (2001) (holding "privacy concerns give way when balanced against the interest in publishing matters of public importance.").

162. Solove, *Taxonomy*, *supra* note 13, at 507.

163. Citizens United v. FEC, 130 S. Ct. 876, 898 (2010).

164. Cent. Hudson Gas v. Pub. Serv. Comm'n, 447 U.S. 557, 562–63 (1980) ("The Constitution therefore accords a lesser protection to commercial speech than to other constitutionally guaranteed expression.") (citing Ohralik v. Ohio State Bar Assn., 436 U.S. 447, 456, 457 (1978)).

ceives the highest First Amendment protection).[165] In the past, courts have treated the collection and dissemination of voter data by pollsters as political speech, protected under the First Amendment.[166] Other courts have casually dealt with data as speech, relying heavily on a "slippage between images of information as speech and as (owned and traded) commodity . . . ."[167] But regulation of other information markets, such as securities, intellectual property, and computer crimes, is permissible under the First Amendment.[168] Many restrictions on political speech have been upheld under strict scrutiny.[169] Nevertheless, "[p]rivacy rules punishing or preventing the dissemination of truthful information have long been perceived as threatening core First Amendment values . . . ."[170]

2. Theories and Proposals to Protect Data Privacy

Under a property rights conception of privacy, the key question is to whom personal data belongs; operators of databases argue that they "own" the data,[171] while some privacy advocates argue individuals should be allowed to buy and sell their own personal information.[172] Another approach would seek to maximize the freedom of various actors to choose the disposition of their data.[173] A third approach argues that "the collection and processing of personal data creates knowledge,"

---

165. *Citizens United*, 130 S. Ct. at 898 ("The First Amendment 'has its fullest and most urgent application' to speech uttered during a campaign for political office.") (quoting Eu v. S.F. County Democratic Central Comm., 489 U.S. 214, 223 (1989)).

166. *E.g.*, Nat'l Broad. Co. v. Colburg, 699 F. Supp. 241, 242 (D. Mont. 1988) ("Gathering and dissemination of information concerning why and how people vote constitutes speech which is protected by the first amendment.").

167. Cohen, *Examined Lives*, *supra* note 8, at 1413–14.

168. *Id.* at 1416–17; *see also* Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650, 1653 (2009) (discussing the "tension between these two very different First Amendment regimes for civil liability" in torts versus contract and property claims).

169. *E.g.*, Stretton v. Disciplinary Bd. of Supreme Court of Pa., 944 F.2d 137, 139 (3rd Cir. 1991) (upholding prohibitions against judicial candidates "announcing their views on disputed legal or political issues" and soliciting campaign contributions).

170. Richards, *supra* note 74, at 1119.

171. Cohen, *Examined Lives*, *supra* note 8, at 1378 ("Opponents of strengthened privacy protection . . . point to their investment in compiling the databases and developing algorithms to "mine" them for various purposes.").

172. *Id.*

173. *Id.* at 1391–92 ("What matters most is that personal data is owned at the end of the day in the manner the parties have agreed.").

and marketers armed with this knowledge are better able to serve consumers.[174] A fourth approach looks at the relationship between data and speech, and concludes that privacy "interfere[s] with the speech rights of would-be data-collectors to spread any judgments, generalizations, and correlations that are salable and not demonstrably false."[175]

The most recent attempts at privacy reform in the United States focus on notice and consent—whether individuals "fully understand and appreciate what information is being collected about them, and whether or not they are empowered to stop certain practices from taking place."[176] The Commercial Privacy Bill of Rights Act, proposed in April 2011, would create a broader privacy law than those currently enacted and allow consumers to access data about themselves and block some uses of it.[177] The White House's Consumer Privacy Bill of Rights establishes a framework for data privacy based on individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.[178] This approach most closely resembles the freedom of choice theory.

Absent new restrictions on political data-mining, the low cost and easy availability of political information such as voter registration, voting history, and campaign contributions, may actually slow (but not stop) the erosion of privacy. If a campaign can easily access such data through government websites, and then manage the data on increasingly powerful personal computers with common software such as Excel or Access, it might choose to spend more on television buys and hire a part-time (or volunteer) in-house data manager to query the data for likely voters and donors rather than hiring a data firm. A campaign could potentially hand the job of downloading

---

174. *Id.* at 1402.

175. *Id.* at 1409.

176. *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci. and Transp.*, 111th Cong. (2010) (statement of Sen. John D. Rockefeller IV, Chairman, S. Comm. on Commerce, Sci. & Transp.), *available at* http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=0bfb9dfc-bbd7-40d6-8467-3b3344c72235&Statement_id=21f3326d-345f-4aaa-b105-0532997b481e&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2010 (last visited Feb. 26, 2012).

177. Julia Angwin, *Senators Offer Privacy Bill to Protect Personal Data*, WALL ST. J, April 13, 2011, at B1.

178. WHITE HOUSE, *supra* note 72, at 47–48.

voter rolls and campaign finance reports to a volunteer and not even bother raising the money that would have been spent on a data firm. The candidate might spend less time in the call room raising money and more time on voter contact. The mark-up for data consultants may decrease along with the demand for their services. Unregulated, the political information trade could cease to be so lucrative as it becomes democratized.[179] Still, the aggregation of consumer data with political data would remain a powerful tool—especially for statewide and federal campaigns. However, easy access to political data means more campaigns have the opportunity to breach voter privacy.[180]

Some proposed remedies to political data protection problems are overly restrictive, under-protective, or both. Johnson et al. recommend making donor data "read only" to increase the cost of importing such data into political databases.[181] This would seem to only bar outsider candidates with limited resources from using the data, while professional political data-miners will quickly find a way to work around the nuisance—making their service even more valuable.[182] They also propose limiting the lifespan of contributor data, but again, professional data-miners could quickly find a work-around and mark-up the cost of their services. One possibility for reform would be to prohibit the processing of data revealing political beliefs, as the EU directive does.[183] Such an approach may or may not be permissible under the First Amendment.[184] But a broad prohibition would foreclose the benefits of political data-mining,

---

179. *Cf.* Hardy, *supra* note 93 (remarking that "Big Data" is a big business with "an uncountable number of data-mining startups in the field").

180. Further, a Senator in Washington, D.C. likely has less interest in an individual's political leanings than does a city councilperson next door. Access to political information by personal acquaintances may actually have a greater impact on an individual's life than access by a national political figure.

181. Deborah G. Johnson, et al., *Campaign Disclosure, Privacy, and Transparency*, 19 WM. & MARY BILL RTS. J. 959, 980 (2011).

182. Part of Aristotle's appeal for many years has been its data gathered from hard-to-get public sources, "located on ledgers or computers in town halls, state office buildings or county courthouses, each with different hours and different rules of access." Wayne, *supra* note 7, A10.

183. EU DIRECTIVE, *supra* note 76, at art. 8 ("Member States shall prohibit the processing of personal data revealing . . . political opinions . . . ."). The Directive goes on to carve out exceptions, including one for non-profits with political purposes. *Id.*

184. *See* Solove & Richards, *supra* note 168, at 1652–53 (discussing the duality of the law's approach to civil liability when the First Amendment is implicated).

namely increasing voter turnout. Mandatory disclosure of data-mining activities would be a narrower approach to protecting voter autonomy.

B. MANDATORY DISCLOSURE TO PROTECT VOTER AUTONOMY

A successful voter privacy policy must satisfy three general privacy constraints: (1) balancing free speech with ownership, (2) providing meaningful notice and consent, and (3) holding data-miners accountable to individuals and society.[185] The ultimate goal must be to preserve intellectual "breathing room" in which voters can autonomously make political choices.[186]

1. Requiring Campaigns to Disclose Voter Profiles to Individual Voters

Campaigns should be required to disclose their data-mining activity. Additionally, voters should be allowed to request their own profile from federal-level campaigns, and campaigns should have to disclose their use of outside databases. Voters should then be allowed to choose to opt out of profiling. However voters would not be permitted to opt out of receiving political ads. This approach would create only a minimal burden (if any) on campaign speech, while protecting the property rights of both individuals and data-miners. It would give adequate notice and opportunity for consent to voters, and it would bring political data-mining into public view, where voters and consumers would be better situated to hold data-miners accountable.

2. Constitutionality of Disclosure

The highest legal hurdle for any proposal to reform voter privacy is the First Amendment. Political speech is core protected speech under the First Amendment, and laws limiting such speech must be able to withstand strict scrutiny by courts.[187] To do so, the law must "further[] a compelling inter-

---

185. Cohen, *Examined Lives*, *supra* note 8, at 1428.

186. Richards, *supra* note 74, at 1120 ("By protecting sheltered intellectual exploration and the processes by which opinions and ideas are generated, data privacy rules create expressive breathing room and intellectual autonomy and could themselves be viewed as having First Amendment magnitude.").

187. *Citizens United*, 130 S. Ct. at 898 ("[P]olitical speech must prevail against laws that would suppress it, whether by design or inadvertence.").

est and [be] narrowly tailored to achieve that interest."[188] A proposal that instead limits commercial speech would undergo less exacting scrutiny under the *Central Hudson* test.[189] Any limitation on commercial speech must directly advance a substantial government interest by means no more expansive than necessary.[190] A proposal that does not limit speech will not invoke First Amendment protections.

A voter profile disclosure law could survive strict scrutiny, so the question of what type of speech it restricts is moot. The compelling government interest advanced by the proposal is voter privacy. The D.C. Circuit Court found the FEC's prohibition on use of contribution data for fundraising purposes to serve an important government interest, but the interest was in the value of the donor list to the campaign, not in the privacy of the donors.[191] Nevertheless, voter privacy and autonomy would likely be perceived as compelling government interests. Disclosure advances the interest by revealing the sources of the voter's data trail. The opt-out provision would protect privacy by giving voters control over their own personal information. To determine whether the disclosure of profile data is narrowly tailored, courts will examine whether the law restricts speech no more than necessary to advance its interests. The Supreme Court has found that "[d]isclaimer and disclosure requirements may burden the ability to speak, but they 'impose no ceiling on campaign-related activities,' and 'do not prevent anyone from speaking.'"[192] This disclosure requirement would place minimal burdens on a campaign's speech; to satisfy the disclosure requirement, all a campaign would need is an interface on its website for voters to enter their name and address (or perhaps a more secure username and password) to view their own digital dossier. The log-in procedure would make mining data from the interface too burdensome for other data-miners to ex-

188. Federal Election Comm'n v. Wisconsin Right to Life, Inc., 551 U.S. 449, 464 (2007).

189. *Central Hudson*, 447 U.S. at 562–63 ("The Constitution therefore accords a lesser protection to commercial speech than to other constitutionally guaranteed expression.").

190. *Id.* at 564 ("The State must assert a substantial interest . . . the restriction must directly advance the state interest," and "if the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.").

191. Johnson et al., *supra* note 181, at 966 (2011).

192. *Citizens United*, 130 S. Ct. at 914 (2010) (quoting Buckley v. Valeo, 424 U.S. 1 at 64 (1976) and McConnell v. FEC, 540 U.S. 93 at 201 (2003)).

ploit,[193] so private data-miners' business would be protected. Further, the Court favors opt-out provisions over opt-in.[194] More restrictive means of protecting privacy are imaginable but may be impermissible under the First Amendment; banning some or all political data-mining would seriously impede speech, as would an opt-in provision.

3. Application

To be effective, the disclosure requirement would have to apply to campaigns at both the state and federal level, including PACs and groups campaigning for referendums. At the same time, placing burdens on low-visibility state and local races could deter cash-strapped candidates from entering races, so the requirement should only apply above a threshold spending level. The provision could be adopted either as part of general election law, or it could be made a condition of accepting public campaign financing.

IV. CONCLUSION

When a citizen's privacy is breached by political data-mining, there is typically no villain behind the act.[195] Politicians hire data firms to win elections, so data consultants are in fact playing a positive role in public service: by identifying voting patterns based on consumer data, campaigns can appeal to individuals who have not previously voted, thereby increasing voter turnout.[196] With no clear tortfeasor, fighting breaches of privacy is nearly impossible. Nevertheless, the privacy inter-

193. Unlike the protections envisioned by Johnson et al., voters would only be able to view one record at a time—their own. *Cf.* Johnson et al., *supra* note 181, at 978.

194. Reno v. Am. Civil Liberties Union, 521 U.S. 844, (1997). *See also* Cohen v. California, 403 U.S. 15, 21 (1971) (noting bystanders to offensive speech could opt out "simply by averting their eyes") "The ability of government, consonant with the Constitution, to shut off discourse solely to protect others from hearing it is, in other words, dependent upon a showing that substantial privacy interests are being invaded in an essentially intolerable manner." *Id.* By not permitting voters to opt out of receiving political advertisements, the law skirts a First Amendment challenge to restricting political advertising.

195. Solove, *Taxonomy*, *supra* note 13, at 559 ("In many instances, there is no clear-cut wrongdoer, no indisputable villain whose activities lack social value.").

196. *See* Kreiss, *supra* note 143, at 72 ("The Obama campaign targeted priority individuals residing in heavily Republican districts, and focused on neighborhoods with low voter turnout but high numbers of likely supporters.").

ests of citizens must be balanced against other valid rights and not simply dismissed. First Amendment protections are themselves driven partly by concerns over autonomy and self-government—the same concerns underlying the right to privacy. Personally identifiable data is now being constantly recorded and used in remarkable ways that can increase efficiency for vendors, decrease the cost of running an effective campaign for political candidates, and connect voters with candidates who suit their tastes and preferences. Political data-mining comes with economic and social benefits, and suppressing information collection would be onerous and counterproductive. Adhering to the principles of the Consumer Privacy Bill of Rights, voter privacy remedies should acknowledge the value of political data-mining and focus on empowering voters to exercise control over their personal information.