Arkansas Law Review

Volume 70 | Number 3 Article 6

December 2017

Civil Society and Cybersurveillance

Andrew McCanse Wright
Savannah Law School

CIVIL SOCIETY AND CYBERSURVEILLANCE

Andrew McCanse Wright*

I. INTRODUCTION

There is no such thing as benign surveillance.[1] It always comes with costs because of the chill it visits upon conduct, education, associations, and expression.[2] Government surveillance has been magnified by cybersurveillance[3] in the Digital Age[4] to a degree unimaginable by the Founders of the United States of America.[5] The various National Security

* Associate Professor, Savannah Law School. I wrote this essay for presentation at the Cybersurveillance Discussion Forum held at the Université Paris-Dauphine. I am grateful and indebted to Russ Weaver and the other Forum hosts and participants. I would also like to thank Vinay Harpalani, Ron Krotoszynski, Caprice Roberts, and Gary Wright for their thoughtful comments on earlier drafts. Finally, Erica Drew, Katelyn Ashton, and Meagan Rafferty provided invaluable research and editorial support.

1. Surveillance is commonly associated with law enforcement. *See, e.g.*, *Surveillance*, CAMBRIDGE ACADEMIC CONTENT DICTIONARY (1st ed. 2009) (defining "surveillance" as "the act of watching a person or a place, especially a person believed to be involved with criminal activity or a place where criminals gather"). While that connotation has relevance to this essay, I use "surveillance" to refer to "the gathering and analysis of information in the pursuit of various finalities—in particular, preventing certain risks, orienting human behaviors and, in the event of a problem, locating the persons responsible." Monica Tremblay, *Cyber-Surveillance*, *in* THE ENCYCLOPEDIC DICTIONARY OF PUBLIC ADMINISTRATION (L. Côté & J.-F. Savard eds., online ed. 2012), http://www.dictionnaire.enap.ca/dictionnaire/docs/definitions/definitions_anglais/cyber_surveillance.pdf [https://perma.cc/62YN-QUM5]; *see also* DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 14 (2007) (defining surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction").

2. Surveillance provides public and private benefits as well, but the fact that observation affects those aware of its potential is manifest. *See infra* Part V.

3. I use the term "cybersurveillance" as defined in the *Encyclopedic Dictionary of Public Administration* because it encompasses technical platforms beyond the Internet: "a mechanism for the surveillance of persons, objects or processes that is based on new technologies and that is operated from and on data networks, such as the Internet." Tremblay, *supra* note 1.

4. I refer to the "Digital Age," also called the Information Age, as the time period starting in the 1970s and defined by the introduction of the personal computer and subsequent technology that allows the rapid and massive storage and transfer of information in digital form. *See Digital Age*, CAMBRIDGE BUSINESS ENGLISH DICTIONARY (2011).

5. While some of these observations would apply to the European Union, the Commonwealth, and other comparative contexts, I address these questions through the lens

Agency (NSA) telephone and internet surveillance programs that have come to light[6] shocked the public as a matter of scale and audacity.[7] There has also been a raging debate about government access to counter-surveillance encryption technology.[8]

However, the entry of government cybersurveillance into the daily routines of life may pose an even greater concern. The unfolding technological revolution profoundly alters human relations to governments, business entities, civic institutions, and social associations.[9] As the world becomes more interconnected, national security threats can grow domestically, cross physical borders, or emanate from digital space itself.[10] At the same time, government surveillance-capacity expansion has been geometric.[11] All of these developments threaten private spaces

---

of the American constitutional system.

6. *See* LUKE HARDING, THE SNOWDEN FILES: THE INSIDE STORY OF THE WORLD'S MOST WANTED MAN 10-11 (2014); Dustin Volz, *Everything We Learned from Edward Snowden in 2013*, NAT'L J. (Dec. 31, 2013). For a pre-Snowden perspective, *see* Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 STAN. L. REV. 1023, 1032-35 (2008) (outlining public reporting about the NSA surveillance program).

7. As the invitation to the 2016 Privacy Forum indicates: "[T]he size of the NSA surveillance and collection program was absolutely staggering, with the NSA spending some $10.8 billion per year and maintaining a staff of some 35,000 employees." Russel L. Weaver & Laurence Boissier, *Governmental Transparency and Openness in a Digital Era: A U.S. Perspective*, 2 INT'L J. DIGITAL & DATA L. 59, 69 (2016) (footnotes omitted) (discussing the government's large cybersurveillance operation and how if not for Edward Snowden "the American people might never have known about [its] size").

8. *Compare* James B. Comey, Director, Fed. Bureau Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Remarks at the Brookings Institution (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/4GS9-2WEG] (arguing to extend to emerging technologies those legal requirements for telecommunications carriers and broadband providers to build interception capabilities into their networks for court-ordered surveillance), *with* Rob Price, *Tim Cook's Internal Memo to All Apple Employees on the Company's Fight Against the FBI*, BUS. INSIDER (Feb. 22, 2016, 7:14 AM), http://www.businessinsider.com/tim-cook-apple-fbi-hack-iphone-san-bernardino-memo-2016-2 [https://perma.cc/5ECL-H6VX] (thanking employees for supporting Apple's opposition to the FBI's request to order a workaround of the encryption on the San Bernardino terrorism suspect's iPhones because "we use encryption to protect our customers—whose data is under siege").

9. *See infra* Part VI.

10. KRISTIN FINKLEA & CATHERINE A. THEOHARY, CONG. RESEARCH SERV., REP. NO. R42547, CYBERCRIME: CONCEPTUAL ISSUES FOR CONGRESS AND U.S. LAW ENFORCEMENT 8 (2015).

11. *See infra* Part VI.

and modes that are essential to self-government.[12]

In this essay, I argue that it would be productive to reverse prevailing thought about privacy and government surveillance. Traditional legal analysis calls on courts and policy makers to look to specific provisions of governmental charters and laws to address the permissibility of a particular government surveillance effort.[13] Rather, courts and policy makers would benefit from assessing the freedom from surveillance required to preserve an empowered democratic citizenry and working backwards to assess whether a particular government surveillance effort stifles that freedom.

The United States was established as a liberal democratic republic.[14] One of the essential features of the American political scheme is a civil society, which presupposes "a social sphere separate from both the state and the market."[15] It requires apartness from the government. That separation from the government, which I will call the *civil preserve*,[16] is a necessary feature for both legitimate government (i.e., the consent of the governed) as well as democratic self-government (i.e., empowered citizens). Beyond the sequential approach of classic Fourth Amendment analysis,[17] civil society theory raises other

---

12. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1267-68 (2004).

13. *Id.* at 1267, 1269-76.

14. *See* PERRY KELLY, EUROPEAN AND INTERNATIONAL MEDIA LAW: LIBERAL DEMOCRACY, TRADE, AND THE NEW MEDIA 57 (2011) (describing the "early American start as an avowedly liberal democratic republic"). The United States is "liberal" in that it protects civil liberties and political freedom by means of the rule of law and constitutional limitation, "democratic" in that American citizens elect their leaders, and "republican" in that policy decisions are primarily made by elected leaders. *See generally* RONALD DWORKIN, A MATTER OF PRINCIPLE (1985).

15. ALISON MACK ET AL., NAT'L ACADS. OF SCIS., ENG'G & MED., GLOBAL HEALTH RISK FRAMEWORK: GOVERNANCE FOR GLOBAL HEALTH: WORKSHOP SUMMARY 112 (2016). For a more fulsome discussion of various definitions and underpinnings of civil society theory, see Benny D. Setianto, *Somewhere in Between: Conceptualizing Civil Society*, 10 INT'L J. OF NOT-FOR-PROFIT L. 109, 110, 113-17 (2007).

16. The term "civil preserve" has been used to denote the area of authority held exclusively by the President of the United States in relation to subordinate military commanders. *See, e.g.*, JAMES A. RAWLEY, TURNING POINTS OF THE CIVIL WAR 173-74 (New Bison Books ed., Univ. of Neb. Press 1989) (1966) (describing politics as part of "the civil preserve of the President, not to be poached on by a general"). I appropriate the term as used differently in this essay but adopt the concept of an area not to be encroached upon.

17. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315-16 (2012) ("The sequential approach is not merely a minor aspect of Fourth

fundamental questions.[18] What kind of citizen do we need? What zone of autonomy is necessary to build that kind of citizen? In a more aggregate sense, what space is required to create private associations that build the political culture necessary for government by the people?

Benjamin Franklin famously wrote: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."[19] The civil preserve consists of essential liberty and privacy. Protection of the civil preserve should be the paramount limitation on public interests in cybersurveillance as a means of countering criminal activity and national security threats. At first blush, the civil preserve does not readily lend itself to practical judicial processes. But an understanding of its essence, attributes, and limitations should be a central concern to academics, policy makers, and judges.

II. CIVIL SOCIETY THEORY

Civil society is a defining feature of the American liberal democratic republic.[20] In one sense, the American system can be defined in the negative. The theory divides the world into public and private spaces, with a "society" in the middle that mediates between the public and private spheres. As one commentator notes:

> [C]ivil society denotes those collectivities, or those collective actions and norms, which are outside of and autonomous from the state, being also neither the property of the 'private sphere' (of family life) or of the economy (whether or not the economy is defined as 'private'). Civil

Amendment doctrine. Rather, it forms the foundation of existing search and seizure analysis.").

18. *See infra* Part II.

19. CARLA J. MULFORD, BENJAMIN FRANKLIN AND THE ENDS OF EMPIRE 178 (2015) (observing that Franklin's quotation "has consonance with some of the most important articulations about liberty and governance in early modern liberal expression"). *But see* Benjamin Wittes, *What Ben Franklin Really Said*, LAWFARE (July 15, 2011, 6:53 AM), https://www.lawfareblog.com/what-ben-franklin-really-said#.UvvR12RDtZs [https://perma.cc/6H43-QRTL] ("In other words, the 'essential liberty' to which Franklin referred was thus not what we would think of today as civil liberties but, rather, the right of self-governance of a legislature in the interests of collective security.").

20. Gideon B. Baker, Civil Society and Democratisation Theory: An Inter-Regional Comparison 1 (Sept. 1998) (unpublished D. Phil. dissertation, University of Leeds), https://core.ac.uk/download/pdf/43716.pdf [https://perma.cc/9KE2-4ARE].

> society is therefore at once public and private—'public' in the sense that human association always has implications for the wider community, placing an individual in a particular relation to others and to the whole; and 'private' in that it falls outside of the formal political sphere where publicly binding decisions are made. Of course, both the family and the economy also posses [sic] these characteristics, yet civil society is defined apart from these constructs because it is in some ways (or ideally) a realm of voluntary association.[21]

It is in this sense that a "society" dwells in that middle space. These voluntary associations are mediating institutions upon which the broader American political system relies.[22] Mediating institutions help create the attributes necessary for democratic citizenship.[23]

The space reserved for people apart from government is apparent when compared to the totalitarian theory[24] of Communism guiding the Democratic People's Republic of

---

21. *Id.* at 20; *see also* Michael W. Foley & Bob Edwards, *Beyond Tocqueville: Civil Society and Social Capital in Comparative Perspective*, 42 AM. BEHAVIORAL SCIENTIST 5, 6 (1998) (tracing the modern usage of the term "civil society" to "the 18th-century effort to wrest a social space within which emerging and preexisting types of associations could pursue their own ends relatively free from the absolutizing pretensions of both monarchists and radical republicans").

22. *See* Steven G. Calabresi, *Political Parties as Mediating Institutions*, 61 U. CHI. L. REV. 1479, 1490 (1994) (characterizing synagogues, churches, temples, families, and voluntary community and civic associations as "mediating institutions [that] may truly mediate between the private individual and the state") (citing ALEXIS DE TOCQUEVILLE, 1 DEMOCRACY IN AMERICA 310-34 (Henry Reeve, trans., Vintage Books 1945) (1835)).

23. *See* Foley & Edwards, *supra* note 21, at 11-12 (theorizing that civil society's mediating institutions perform socialization functions, quasi-public functions, and representative functions for civic culture).

24. A totalitarian government recognizes no limits to its power and no autonomy in its populace. It claims not just a monopoly on political power, but the regulation of all *cultural*, religious, and economic elements of society. Giovanni Amendola first articulated "total" state power as a description of Italian Fascism. *See* RICHARD PIPES, RUSSIA UNDER THE BOLSHEVIK REGIME 243 (1993). On his path to Nazism, a Weimar Republic jurist coined the term *Totalstaat*. *See* CARL SCHMITT, THE CONCEPT OF THE POLITICAL 22 (George Schwab trans., Rutgers Univ. Press 1976) (1932); *see also* HANNAH ARENDT, THE ORIGINS OF TOTALITARIANISM 307-11 (new ed. 1973) (describing ideology as the engine and organizing principle of the totalitarian regime).

Korea[25] or the theocracy model[26] aspired to by the Islamic Republic of Iran.[27] The United States was formed on a theory of consent of the governed rather than a claim of divine mandate.[28] America's Founders radically departed from the *ancien régime* by conferring government legitimacy by means of a voting franchise.[29] Since that time, the United States has extended those rights, albeit fitfully, to freedmen, people who could not afford a

25. Changyong Choi, *"Everyday Politics" in North Korea*, 72 J. ASIAN STUD. 655, 656 (2013) ("Many studies have focused on North Korea as a socialist state and the fact that its political system is based on highly structured totalitarianism, where collective rules and political and ideological solidarity are emphasized over individual activities.") (citations omitted).

26. In a theocracy, "God is recognized as the immediate ruler and His laws are taken as the legal code of the community and are expounded and administered by holy men as His agents." S.E.F., *Theocracy*, *in* THE BLACKWELL ENCYCLOPAEDIA OF POLITICAL INSTITUTIONS 610 (Vernon Bogdanor ed., 1987). A theocracy can be defined as a totalitarian state in which the governing ideology is the concept of one true religion that regulates political, cultural, and economic elements of society. *See* Mario Ferrero, *The Rise and Demise of Theocracy: Theory and Some Evidence*, 156 PUB. CHOICE 723, 723-24 (2013)("Theocracy literally means government by God . . . . [T]he word in its strict sense is usually understood to mean government by a clergy, or a self-appointed group who claim to speak and act on God's behalf.").

27. *See* H. E. Chehabi, *Religion and Politics in Iran: How Theocratic is the Islamic Republic?*, 120 DAEDALUS 69, 72-74 (1991) (detailing Ayatollah Khameini's fitful revolution project to subsume Iran's political, legal, social and economic life under the theocratic control of clerics). Iran's political regime is particularly complicated, with multiple power centers and some democratic processes that dilute the Ayatollah's theocratic claims. *See* Stephen C. Fairbanks, *Theocracy Versus Democracy: Iran Considers Political Parties*, 52 MIDDLE EAST J. 17, 31 (1998) ("Khatami's 20 million voters ushered in a principle of people's government and a demand for the institutions of civil society. Those ideas are difficult to reconcile with theocracy . . . .").

28. U.S. CONST. pmbl. (declaring "We the People . . . ordain[ed] and establish[ed]" the U.S. Constitution). "The first three words of the preamble to the Constitution suggest one element unique to the American Revolution: its outcome was a government created by the people, not one existing independently of them . . . ." Donald L. Doernberg, *"We the People": John Locke, Collective Constitutional Rights, and Standing to Challenge Government Action*, 73 CAL. L. REV. 52, 52 (1985) (footnote omitted); *see also* JOHN RAWLS, A THEORY OF JUSTICE 118-23 (Belknap Press rev. ed. 1999) (1971) (arguing the legitimacy of a social contract depends on free and rational choice by all individuals in the original position, in which each person's preferences are separated by a "veil of ignorance"); Michel Rosenfeld, *Contract and Justice: The Relation Between Classical Contract Law and Social Contract Theory*, 70 IOWA L. REV. 769, 847-80 (1985) (summarizing the various social contract theories of Thomas Hobbes, John Locke, Jean Jacque Rousseau, and Immanuel Kant that a social contract is a set of collectively binding social arrangements predicated on consent of those governed by it).

29. *See* ALEXANDER KEYSSAR, THE RIGHT TO VOTE: THE CONTESTED HISTORY OF DEMOCRACY IN THE UNITED STATES 8-9 (2000).

poll tax, women, and those eighteen years old.[30] Notwithstanding more recent conservative efforts to curtail ballot access[31] and uneven Supreme Court election law jurisprudence,[32] voting remains central to the legitimacy of American government.

The American model requires a dedicated private sphere and a robust civil society. A civil preserve is essential to create the space necessary to participate in mediating institutions and maintain the tools of self-government. However, the ruthless efficiency and expansion of cybersurveillance often intrudes upon behavior reflecting private conscience and voluntary association.[33]

III. THE CIVIL PRESERVE

A civil preserve is defined by the privacy and liberty that allow for autonomy required of citizens in a system of self-government. Citizens in a liberal democratic republic have governing responsibilities.[34] Formally, they may vote, petition the government, determine probable cause, and find legal facts.[35] However, a polity must create the conditions necessary for a

30. *See* Kenneth T. Walsh, *Voting Rights Still a Hot-Button Issue*, U.S. NEWS (Aug. 4, 2015, 12:01 AM), https://www.usnews.com/news/articles/2015/08/04/voting-rights-still-a-political-issue-50-years-later [https://perma.cc/PL5N-995u].

31. *See* William D. Hicks et al., *A Principle or a Strategy? Voter Identification Laws and Partisan Competition in the American States*, 68 POL. RES. Q. 18, 19-21 (2015) (finding that Republican-controlled legislatures strongly influence the adoption of voter identification laws in electorally competitive states as a partisan countermeasure to a demographically declining electoral coalition); *see also* Ari Berman, *The GOP War on Voting*, ROLLING STONE (Aug. 30, 2011), http://www.rollingstone.com/politics/news/the-gop-war-on-voting-20110830 [https://perma.cc/C5U5-4Z4K] (discussing efforts by prominent conservatives, including Paul Weyrich, David Koch, Charles Koch, to push election reforms that restrict voter access for partisan gain).

32. Joshua A. Douglas, *A Pivotal Moment for Election Law*, 104 KY. L.J. 547, 559 (2016) ("Reforming the Court's election law jurisprudence could result in a better functioning democratic process; entrenching or extending harmful precedents will impede that goal.").

33. *See*, *e.g.*, People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.").

34. *Citizenship Rights and Responsibilities*, U.S. CITIZENSHIP & IMMIGRATION SERVS., https://www.uscis.gov/citizenship/learners/citizenship-rights-and-responsibilities [https://perma.cc/XVX7-V5KB].

35. *Id.*

populace to effectively fulfill those formal functions.

Much has been written about the process of citizen creation since Alexis de Tocqueville published his findings in *Democracy in America*,[36] including the importance of mediating institutions and the role of enlightened self-interest.[37] These are the building blocks of the American system, and they rely on autonomous and empowered citizens. Citizens need to educate themselves about issues because it is critical for citizens to cast votes on matters of public importance. The populace needs space to develop private conscience and public virtues. Citizens need to be able to inculcate those values in their children and charges. They must rely on a free flow of information in a marketplace of ideas that sits apart from government-issued messages. There must be room for brainstorms and dissent. In order to organize politically, people need freedom to associate and build coalitions. They need to be able to communicate messages that contradict, and even disdain, government policy. At the same time, citizens must observe the rule of law and develop a healthy respect for government authority. They respect authority by adhering to the rule of law in deference to its legitimacy.[38] In sum, citizens need to be legally obedient but politically and culturally autonomous.

The civil preserve is analogous to the zone of branch autonomy required to perform essential functions that are the touchstone of a functionalist's approach to separation of powers.[39] The civil preserve constitutes the autonomous zone for

36. *See generally* ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA (J.P. Mayer & Max Lerner eds., George Lawrence, trans., Harper & Row 1966) (1835).

37. Tocqueville believed American participation in voluntary associations organized around common interests or political issues created an enlightened self-interest. He argued they had a transformational effect: "At first it is of necessity that men attend to the public interest, afterward by choice. What had been calculation becomes instinct. By dint of working for the good of his fellow citizens, he in the end acquires a habit and taste for serving them." *Id*. at 484.

38. *See generally* TOM R. TYLER, WHY PEOPLE OBEY THE LAW (2006) (emphasizing empirical evidence that legitimacy, when compared to deterrence, is a salient motivator of law obedience).

39. *See, e.g.*, M. Elizabeth Magill, *Beyond Powers and Branches in Separation of Powers Law*, 150 U. PA. L. REV. 603, 611 (2001) (noting the view that "the flexibility . . . evaporates if the arrangement threatens 'core' functions"); Peter L. Strauss, *Formal and Functional Approaches to Separation-of-Powers Questions—A Foolish Inconsistency?*, 72 CORNELL L. REV. 488, 489 (1987) (observing "a functional approach . . . stresses core function and relationship, and permits a good deal of flexibility when these attributes are not threatened").

which intrusion stifles the core functions of citizenship. Thus, privacy is both an end and a means.[40] Some degree of privacy is a basic human right.[41] But preservation of a private sphere is also an essential ingredient in democracy.[42] In his book, *Privacy Revisited*, Professor Ronald Krotoszynksi makes compelling observations about the essential relation between democracy and privacy.[43] Without unsurveilled spaces for thoughts, associations, and communications, the people lose their deliberative capacity and institutional independence.

How much privacy do we need to create the apartness necessary to create democratic stewardship of the state rather than subservience to it? It is a vexing question that is not readily susceptible to judicial standards. However, that does not mean the civil preserve is wholly unknowable. While the civil preserve is not a formal part of American constitutional doctrine, U.S. Supreme Court opinions occasionally reference interests that are features of it.[44] Moreover, while the Bill of Rights and Civil War amendments provide a great deal of protection for the civil preserve, they are distinct and not coextensive with it.

IV. THE CIVIL PRESERVE AND THE U.S. CONSTITUTION

The choice to establish the United States as a liberal democratic republic sounding in civil society and ordered liberty contemplates the civil preserve. Perhaps the civil preserve is included among natural rights and therefore preexisted the

40. For a thoughtful treatment of the bundle of concepts associated with privacy, see DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008). As David Pozen notes, privacy interests not only clash with public interests, but also often sit in dynamic tension with other privacy interests. *See* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 221-24 (2016) (citations omitted).

41. James Griffin, *The Human Right to Privacy*, 44 SAN DIEGO L. REV. 697, 700 (2007) ("Without privacy, autonomy is threatened.").

42. *See* Edward F. Ryan, *Privacy, Orthodoxy and Democracy*, 51 CAN. B. REV. 84, 85 (1973).

43. RONALD J. KROTOSZYNKSI, JR., PRIVACY REVISITED: A GLOBAL PERSPECTIVE ON THE RIGHT TO BE LEFT ALONE 175 (2016) ("If speech is integral to democracy and, in turn, privacy in the form of intellectual freedom is integral to speech, then privacy constitutes a necessary condition for the maintenance of democratic self-government.").

44. *See generally* United States v. Jones, 565 U.S. 400 (2012) (analyzing Fourth Amendment jurisprudence and finding that Government committed an unlawful search when it attached a tracking device to Jones's car).

Constitution. After all, the American legal canon begins with the Declaration of Independence's "self-evident" truth that people are "endowed by their Creator with certain unalienable Rights . . . ."[45] Perhaps the civil preserve was implied by the scheme created when "We the People of the United States" ordained and established the Constitution.[46] Maybe the civil preserve is among those rights the Ninth Amendment reminds us are "retained by the people."[47] As Justice Goldberg concluded in his *Griswold v. Connecticut*[48] concurring opinion, "[t]he language and history of the Ninth Amendment reveal that the Framers of the Constitution believed that there are additional fundamental rights, protected from governmental infringement, which exist alongside those fundamental rights specifically mentioned in the first eight constitutional amendments."[49] Under any of these authorities, a civil preserve is *a priori* to the Bill of Rights.[50]

It is one thing to acknowledge the existence and significance of a civil preserve. It is quite another to provide meaningful standards cognizable to legal processes operating in the real world.[51] For the most part, the text and legal doctrine of specific constitutional provisions will do the work. However, there are areas in which structural limitations and the Bill of Rights may be insufficient. Such potentialities are magnified in the context of cybersurveillance in the Digital Age.[52]

Originally, the Federalist Founders opposed the need for a Bill of Rights. In part, they believed the democratic process

45. THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).

46. U.S. CONST. pmbl.

47. U.S. CONST. amend. IX.

48. 381 U.S. 479 (1965).

49. *Id.* at 488 (Goldberg, J., concurring); *see also* Louis Michael Seidman, *Our Unsettled Ninth Amendment: An Essay on Unenumerated Rights and the Impossibility of Textualism*, 98 CAL. L. REV. 2129, 2140 (2010) ("Although [the Ninth Amendment's] scope was limited to the federal government, its intention and effect were to protect individual rights within that scope."). *But see* Russell L. Caplan, *The History and Meaning of the Ninth Amendment*, 69 VA. L. REV. 223, 228 (1983) (arguing that the Ninth Amendment "neither creates new rights nor alters the status of pre-existing rights" but rather "provides that the individual rights contained in state law are to continue in force under the Constitution until modified or eliminated . . . ."); *see also id.* at 243 (stating "[u]nenumerated rights were not federal rights").

50. *See* U.S. CONST. amends. I-X.

51. "The varieties and uncertainties of definition, of course, trouble also attempts to locate privacy in law." Louis Henken, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1419 (1974).

52. *See infra* Part VI.

would safeguard liberty and privacy interests.[53] Additionally, they believed the structural limitations established by a system of separated powers and federalism would limit the federal encroachment on those essential citizen functions,[54] here defined as the civil preserve. However, the politics of national security and the technological pressures of the Digital Age do not seem to be halting the massive expansion of cybersurveillance *vis-à-vis* the civil preserve.[55]

Of course, the Bill of Rights, as extended by the Civil War Amendments, establishes civil liberties that protect aspects of the civil preserve in both rationale and function.[56] The First (expressive, associational, and religious freedom), Third (soldier-quartering prohibition), Fourth (search and seizure protections), Fifth (substantive due process and self-incrimination prohibition), Eighth (punishment limitations), and Fourteenth (due process and incorporation of other provisions to states) Amendments all contain limitations on government power that, collectively, help protect the integrity of the civil preserve.[57] However, the civil preserve is inadequately protected by the sum of these constitutional provisions. The daylight between constitutional provisions and the civil preserve is only exacerbated by Big Data in the Digital Age.

The Fourth Amendment is the natural and primary locus of legal challenges to government cybersurveillance. In the seminal case, *Katz v. United States*, the Supreme Court articulated the Fourth Amendment's reasonable expectation of privacy standard.[58] One of the big problems with American constitutional law regarding the Fourth Amendment is the vulnerability of its reasonable expectation of privacy formulation to a descriptive rather than normative approach. Ever since *Katz*, courts have

53. *See* THE FEDERALIST NO. 84 (Alexander Hamilton) (arguing a bill of rights has "no application to constitutions professedly founded upon the power of the people, and executed by their immediate representatives and servants").

54. *See* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 5 (5th ed. 2015) (noting that some attribute the absence of an "elaborate statement of individual rights in the Constitution" as originally ratified was due to the framers believing it was "unnecessary because rights were adequately protected by the limitations on power of the national government.").

55. *See infra* Part VI.

56. *See* U.S. CONST. amends. I-X.

57. *See id.*

58. 389 U.S. 347, 360-62 (1967) (Harlan, J., concurring).

struggled with the subjective and objective components of a reasonable expectation of privacy that society will recognize.[59] If one were to ask millennial law students whether they believe all their emails and social media are being monitored, many would say "probably." Those diminished privacy expectations are not unfounded.[60] A descriptive view of reasonableness would suggest that the reality of surveillance shrinks society's Fourth Amendment expectations.

Civil society theory counsels for a Fourth Amendment with normative content grounded in democratic notions of ordered liberty.[61] While the Fourth Amendment surely applies to privacy interests beyond those essential for civil society, the reasonableness of one's expectation of privacy must be made in reference to whether the government intrusion pierces the civil preserve. Under this view, Fourth Amendment protections do not constrict based on real world experience or technological capacity, but rather the civil preserve acts as a halo around the citizen that maintains its integrity in each new technological context.

The third-party doctrine vastly expands the reach of government cybersurveillance in the Digital Age.[62] Human interaction with technology is becoming ever more dynamic and

---

59. Russell L. Weaver, *The Fourth Amendment and Technologically Based Surveillance*, 48 Tex. Tech L. Rev. 231, 237 (2015) ("Although the Court has rendered some post-Katz technology decisions that are privacy protective, the general thrust of the Court's jurisprudence has been largely unproductive.").

60. *See, e.g.*, United States v. Graham, 824 F.3d 421, 426-29 (4th Cir. 2016) (en banc) (holding that obtaining historical-cell-site-location information from a Defendant's cell-phone provider was not a Fourth Amendment search under the third-party doctrine); United States v. De L'Isle, 825 F.3d 426, 433 (8th Cir. 2016) (holding police review of magnetic-strip information from the back of credit card does not constitute a Fourth Amendment search); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1313-19 (2012) (outlining the "Death of Privacy" under the headings "The One Device," "The Cloud," "The Social," "Big Data," and "The Surveillance Society"). Ellen Nakashima, *FBI Wants Access to Internet Browser History Without a Warrant in Terrorism and Spy Cases*, WASH. POST (June 6, 2016), https://www.washingtonpost.com/ world/national-security/fbi-wants-access-to-internet-browser-history-without-a-warrant-in-terrorism-and-spy-cases/2016/06/06/2d257328-2c0d-11e6-9de3-6e6e7a14000c_story.html?utm_term=.a009579c170a [https://perma.cc/28Q2-7CSQ].

61. *See generally* Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303 (2010) (arguing that the Fourth Amendment, rather than merely a criminal procedure regulation, is designed to protect political liberty).

62. *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., REP. NO. R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 7 (2014).

central.[63] Convenience and sales discounts create incentives for people to provide massive amounts of information to businesses and service providers.[64] In turn, those entities create enormous commercial databanks that enable them to store, sell, and trade customer information.[65] Third-party doctrine allows the government to obtain all of that information without a warrant. While customers may "voluntarily" provide commercial entities with personal information, it is unlikely they consider whether that information will be provided to the government without giving them an opportunity to object. Under prevailing Fourth Amendment jurisprudence, a person does not have an enforceable privacy interest in information provided to third-party vendors.[66] Concerns about cybersurveillance in the Digital Age motivated Justice Sotomayor to suggest 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."[67] Narrowing the third-party doctrine to construe government collection of nonpublic commercial transaction data as searches requiring warrants supported by probable cause would add prophylaxis for the civil preserve.[68]

---

63. *See* Ray Kurzweil, *The Law of Accelerating Returns*, KURZWEIL ACCELERATING INTELLIGENCE (Mar. 7, 2001), http://www.kurzweilai.net/the-law-of-accelerating-returns [https://perma.cc/STX8-WFUB].

64. *See* Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [https://perma.cc/Y4TL-UB7K].

65. *See* Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 435 (2014) ("While businesses have legitimate reasons to use [customer] data in their day-to-day operations . . . [c]onsumer-oriented legislation should prevent indiscriminate capitalization of data initially divulged for specific transactions . . . .").

66. *See generally* Smith v. Maryland, 442 U.S. 735 (1979) (holding government collection of pen register information from a telephone company does not constitute a Fourth Amendment search because a person does not have a reasonable expectation of privacy in information voluntarily furnished to a third party).

67. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J. concurring) (citing *Smith*, 442 U.S. at 742; United States v. Miller, 425 U.S. 435, 443 (1976)).

68. The Supreme Court will have an opportunity to revisit third-party doctrine in *Carpenter v. United States* during its October 2017 Term. 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402). In *Carpenter*, the FBI, without a warrant, obtained robbery suspects' historical-geolocational information derived from cell phone-to-tower data transmissions, called cell-site-location information or CLSI. *Id.* at 884-85. The Supreme Court granted certiorari on the question of whether the FBI's conduct constitutes a Fourth Amendment "search."

Debate over the "mosaic theory" of the Fourth Amendment[69] might capture the distinction between the privacy interests of the Fourth Amendment and those of the civil preserve. In traditional Fourth Amendment analysis, courts analyze each act alleged to be a search in isolation.[70] Each challenged act is either a Fourth Amendment search or is not, and each search is either reasonable or not.[71] However, under a mosaic theory, a series of government acts of surveillance would be analyzed as a whole to determine whether it reaches a tipping point that would trigger a reasonable expectation of privacy and thus be deemed a search.[72]

Orin Kerr criticizes the mosaic theory as a dramatic departure from traditional Fourth Amendment doctrine, a complication for lower courts to apply and implement in a principled manner, and a disincentive to enact statutory privacy regulations.[73] As D.C. Circuit Judge Sentelle put it in the *Jones* run-up to the Supreme Court: "The sum of an infinite number of zero-value parts is also zero."[74] While Kerr's critique may carry the day as a Fourth Amendment matter, government information mosaics could gravely imperil the civil preserve.

V. THE SURVEILLANCE DISTORTION EFFECT

From devout faith in an omniscient God[75] to the playful

69. *See generally* Kerr, *supra* note 17.

70. *Id*. at 315-16.

71. *See id.*

72. *See id*. at 313 (citing United States v. Maynard, 615 F.3d 544, 562 n.* (D.C. Cir. 2010) (discussing how the court "analyz[ed] "police actions over time").

73. *See id*. at 314-315.

74. United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting).

75. All three major monotheistic religions embrace an all-knowing and watchful conception of God. The Holy Bible contains numerous such verses. *See, e.g.*, *Job* 34:21 (New American Standard) ("For His eyes are upon the ways of a man, And He sees all his steps."); *Matthew* 6:4 (New American Standard) ("[A]nd your Father who sees what is done in secret will reward you."); *1 Chronicles* 28:9 (New American Standard) ("[F]or the Lord searches all hearts, and understands every intent of the thoughts."). The Hebrew Scriptures informing the Jewish faith call the Lord the "God of knowledge" (El De'ot) in 1 *Samuel* 2:3 (New American Standard) and the "Lord Who Sees ("Adonai Yireh") in *Genesis* 22:14 (Tree of Life). In Islam, an Arabic moniker for God is "Al-'Aleem, the '"All-Knowing.'" *See Surah al-An'aam* 6:59 ("And with Him are the keys of the unseen; none knows them except Him. And He knows what is on the land and in the sea. Not a leaf falls but that He knows it.").

childrearing benefit of an ever-watchful Santa Claus,[76] Western societies have presumed that knowledge of observation affects the behavior of the observed. Behavior is most acutely affected where imminent consequences will flow from the observer's knowledge of the target's disfavored conduct. Surveillance is often designed to deter conduct by means of a direct nexus to consequences. English philosopher Jeremy Bentham designed the infamous Panopticon as a jailing facility calculated to regulate inmate behavior by threat of surveillance and sanction.[77] Some have argued that only the specific threat of retaliation creates a chilling effect grounded in surveillance.[78]

However, knowledge of observation, even where consequences are more remote, can still have a distorting effect on autonomy essential to civil society. Professor Krotoszynski observed: "The specter of 'Big Brother' watching will undoubtedly have profound implications for the exercise of expressive freedoms—indeed for the very idea of democracy itself."[79] Ubiquitous surveillance causes distortion effects that could threaten the civil preserve.[80] It could chill expression, research, and associations necessary to maintain popular governance.[81] Surveillance could also adversely affect viewpoint

---

76. *See* JOHN FREDERICK COOTS & HAVEN GILLESPIE, SANTA CLAUS IS COMING TO TOWN (1934) ("He sees you when you're sleepin'; He knows when you're awake; He knows when you've been bad or good; So be good for goodness sake.").

77. *See generally* Jeremy Bentham, *Panopticon, or, The Inspection-House*, *in* 4 THE WORKS OF JEREMY BENTHAM 37-172 (John Bowring ed., 1787). It was designed as a circle by which numerous inmates could be seen by one jailer. While the jailer couldn't monitor all the inmates at once, the inmates could not observe the jailer's attention. Therefore, the chilling effect of potential surveillance generated penal efficiency. Bentham presented it as "[a] new mode of obtaining power of mind over mind, in a quantity hitherto without example . . . ." *Id*. at 39.

78. *See* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 466 (2015) (noting that some commentators "evince skepticism over the effects of surveillance, and suggest that chilling occurs only in response to specific threats of retaliation").

79. Ronald J. Krotoszynski, Jr., *Reconciling Privacy and Speech in the Era of Big Data: A Comparative Legal Analysis*, 56 WM. & MARY L. REV. 1279, 1287 (2015) (footnote omitted).

80. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

81. *See id.* (inviting us to "consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues"). Richards goes on to suggest that information derived from surveillance may be used to exert power through blackmail, manipulation, and discrimination. *See id*. at 1952-

diversity by creating a conformity effect to a degree dangerous to democratic governance.[82] Thus, there is a premium on ensuring that the scope and intrusiveness of surveillance does not so pervade society as to pierce the civil preserve.

VI. CYBERSURVEILLANCE IN THE DIGITAL AGE

In 1971, Justice Douglas declared: "Electronic surveillance is the greatest leveler of human privacy ever known."[83] That case dealt with a motion-to-suppress and testimony by law enforcement obtained by surreptitious radio transmissions and eavesdropping of conversations between the defendant and a government informant.[84] Modern cybersurveillance would be unrecognizable to Justice Douglas in both sophistication and prevalence.

More recently, Justice Sotomayor observed the magnitude of change in her concurring opinion in *United States v. Jones*[85]:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[86]

She raises the specter of cybersurveillance as a threat that could disrupt the relation between citizen and government.

---

58. The government or other actors may use surveillance-derived power to stifle healthy political dissent. *Id.* at 1953.

82. *See* Kaminski & Witnov, *supra* note 78, at 467 (arguing that surveillance retards the development of minority views and promotes conformity with majority views).

83. United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting).

84. *See id.* at 746-47.

85. 565 U.S. 400, 413 (2012). There, the Court held that the warrantless attachment and monitoring of a global positioning system (GPS) tracking device to a vehicle used by a suspect violated the Fourth Amendment. *Id*. at 404. Justice Scalia's majority opinion relied on the physical intrusion of the device as the primary rationale, resurrecting the pre-*Katz* Fourth Amendment doctrine grounded in trespass rather than a reasonable expectation of privacy. *See id.* at 407-10.

86. *Id*. at 416 (Sotomayor, J. concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum J., concurring)).

Seismic changes threaten to shake democratic foundations. Cybersurveillance increases as it becomes cheaper.[87] The cost of data storage has fallen precipitously since the advent of computers.[88] One analysis indicated that the digital storage space that one can purchase per unit of cost has doubled roughly every fourteen months between 1980 and 2009.[89] At the same time, the storage capacity of individual devices has increased; the maximum available disk size for a desktop computer has nearly doubled every eighteen months since 1980.[90] Thus, governments are increasingly able to inexpensively and efficiently store information in bulk.

Another defining feature of the Digital Age is that information is now a commodity to be sold and bartered.[91] Governments[92] and businesses[93] have entered the emergent Big Data[94] markets. Companies collect massive amounts of data

---

87. *See* Drew F. Cohen, *It Costs the Government Just 6.5 Cents an Hour to Spy on You*, POLITICO (Feb. 10, 2014), http://www.politico.com/magazine/story/2014/02/nsa-surveillance-cheap-103335 [https://perma.cc/G8NV-Q4C3].

88. *See* BIG DATA AT WORK: THE DATA SCIENCE REVOLUTION AND ORGANIZATIONAL PSYCHOLOGY 160 (Scott Tonidandel, Eden B. King, & Jose M. Cortina eds., 2015).

89. Matthew Komorowski, *A History of Storage* Cost, MKOMO.COM (Sept. 8, 2009), http://www.mkomo.com/cost-per-gigabyte [https://perma.cc/4WQK-KQL7]; *see also* Matthew Komorowski, *A History of Storage Cost (Update)*, MKOMO.COM (Mar. 9, 2014), http://www.mkomo.com/cost-per-gigabyte-update [https://perma.cc/YDR8-R4QE].

90. Richard Wright et al., *The Significance of Storage in the "Cost of Risk" of Digital Preservation*, 4 INT'L J. DIGITAL CURATION 104, 105 (2009).

91. *See* THE POLITICAL ECONOMY OF INFORMATION 7-8 (Vincent Mosco & Janet Wasko eds., 1988) ("[C]omputer-communication systems . . . measure and monitor information transactions and permit the packaging and repackaging of information into a marketable commodity.").

92. *See* Reno v. Condon, 528 U.S. 141, 143 (2000) (noting that Congress found that many states sold personal information of motor-vehicle-license applicants as a commercial product); JOHN PODESTA ET AL., EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 22-39 (2014), https://www.whitehouse.gov /sites /default /files /docs /big_data_privacy_report_may_1_2014.pdf [https://perma.cc/QB22-CJXG] (outlining public sector management of data).

93. *See* Jason Morris & Ed Lavandera, *Why Big Companies Buy, Sell Your Data*, CNN (Aug. 23, 2012, 3:52 PM), http://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/ [https://perma.cc/VQ34-X72U] (noting that, by 2012, data sales was "a $300 billion-a-year industry"); *see also Building With Big Data*, ECONOMIST (May 26, 2011), http://www.economist.com/node/18741392 [https://perma.cc/76LQ-T28M].

94. Big Data includes "[e]xtremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions." *See Big Data*, OXFORD LIVING DICTIONARIES, https://en.oxforddictionaries.com/definition/big_data [https://perma.cc/LM5X-RAR6]; *see also* Elena Geanina Ularu et al., *Perspectives on Big Data and Big Data Analytics*, 3

about current and potential customers. Also, political campaigns collect massive amounts of information about voters in order to persuade them and get them to the polls.[95] Many "free" services and bargains for consumers come at the cost of granting information provisions and permission to surveil.[96] There is a vast commercial market for information and data integration.[97]

There is a disorienting effect to the commodification of information. Cybersurveillance captures intimate details of one's life in a physical time and place.[98] However, as it is integrated into Big Data networks, the information becomes storable, packagable, and transferable. Cybersurveillance strips information from the physical world and injects it into a virtual one, decontextualized from human experience. In its amorphous virtual form, data challenges many traditional legal paradigms such as jurisdictional boundaries and international borders.[99]

Most importantly, digital technology continues to transform human behavior. In *Riley v. California*,[100] the Supreme Court invalidated a warrantless search of cell phone data incident to an arrest as a violation of the Fourth Amendment's prohibition on unreasonable searches and seizures.[101] Chief Justice John Roberts, on behalf of the eight-justice majority, noted that mobile phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were

---

DATABASE SYS. J. 3, 4 (2012) (outlining IBM's four aspects of Big Data as volume, velocity, variety, and veracity).

95. *See* David W. Nickerson & Todd Rogers, *Political Campaigns and Big Data*, 28 J. ECON. PERSP. 51, 51 (2014) (noting that since 2008 "campaigns have become increasingly reliant on analyzing large and detailed datasets").

96. *See* Joseph W. Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47, 48 (2013) (citation omitted) (referencing a study that indicated "free internet services offer $2,600 in value . . . in exchange for [user] data").

97. PODESTA ET AL., *supra* note 92, at 43-47 (discussing the data-services sector of the economy).

98. *See* Steven I. Friedland, *I Spy: Self-Cybersurveillance and the "Internet of Things"*, 72 WASH. & LEE L. REV. 1459, 1461 (2015) (citation omitted) (noting that cybertechnology "generate[s] personal, even intimate information").

99. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 330 (2015) ("These unique features of data raise important questions about which 'here' and 'there' matter; they call into question the normative significance of longstanding distinctions between what is territorial and what is extraterritorial. Put bluntly, data is destabilizing territoriality doctrine.").

100. 134 S. Ct. 2473 (2014).

101. *Id.* at 2494-95 (referencing U.S. CONST. amend. IV.).

an important feature of human anatomy."[102] The opinion catalogued the marvel of the modern cell phone:

> The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. One of the most notable distinguishing features of modern cell phones is their immense storage capacity.[103]

These devices record our physical movements, our entertainment preferences, our access to information from the Internet, our associational behavior, and our communications across numerous digital platforms.

In addition, people are buying more and more services online.[104] Digital platforms provide ready access to entertainment, gifts, clothing, transportation, real estate, groceries, education, navigation, and service calls. Digital footprints increasingly betray an individual's public and nonpublic political, religious, and intimate activity. All of this information can be the subject of cybersurveillance. And much of it already is.

Government cybersurveillance comes in different forms. The government's ability to observe citizen data ranges from bulk data collection to an individually targeted collection.[105] There is also a distinction between collection and review. The government may collect data in bulk, store it, and then only search it as particular interests arise.

The government may also surveil directly or indirectly.[106] A

---

102. *Id.* at 2484.

103. *Id.* at 2489.

104. *See* Ruth Mantell, *E-Commerce Speeds Up, Hits Record High Share of Retail Sales*, MARKETWATCH (Aug. 15, 2014, 1:45 PM), http://blogs.marketwatch.com /capitolreport /2014 /08 /15 /e-commerce-speeds-up-hits-record-high-share-of-retail-sales/ [https://perma.cc/4NEZ-WT9X] (charting the significant growth in e-commerce sales from 2000 to 2014).

105. *See* RHODRI JEFFREYS-JONES, WE KNOW ALL ABOUT YOU: THE STORY OF SURVEILLANCE IN BRITAIN AND AMERICA 223 (2017) (outlining a recommendation that government interception of information in counterterrorism investigations, "both individual and bulk," should be subject to judicially approved warrants).

106. Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 621 (2003).

warrant to collect a suspect's email correspondence is a classic example of direct government cybersurveillance.[107] Indirect government cybersurveillance refers to government collection of data provided by target individuals to third parties, usually in the context of commercial transactions.[108] The Fourth Amendment third-party doctrine[109] transforms commercially motivated data collection into storage for indirect government cybersurveillance. Therefore, all cybersurveillance—information collected due to government coercion, government observation, commercial interest, or customer convenience—becomes the potential subject of government cybersurveillance.

There is also an important nexus between cybersurveillance and cybersecurity. Both public and private sector Big Data cybersurveillance fruits become vulnerable to cybersecurity threats from hostile governments,[110] criminal elements,[111] or hacktivists.[112] Cybersecurity's potential failure to secure sensitive personal information held by the government presents an additional threat to the civil preserve.

---

107. *See id.*

108. *Id.* ("[I]ndirect government surveillance rules authorize the government to compel providers to conduct surveillance on the government's behalf.").

109. *See supra* Part IV.

110. Russian state interference operations designed to tilt the U.S. presidential election in favor of Donald Trump roiled American politics well beyond 2016. *See* NAT'L INTELLIGENCE COUNCIL, INTELLIGENCE COMMUNITY ASSESSMENT: ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS ii (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [https://perma.cc/RS4K-PJMG]. I am also among some 22 million people whose U.S. national security clearance documentation, including fingerprint images, was stolen by Chinese hackers. *See* Joe Davidson, *One Year After OPM Cybertheft Hit 22 Million: Are You Safer Now?*, WASH. POST (June 8, 2016), https://www.washingtonpost.com/news/powerpost/wp/2016/06/08/one-year-after-opm-cybertheft-hit-22-million-are-you-safer-now/?utm_term=.c8b656ea8482 [https://perma.cc/UV4G-64MJ].

111. *See* FINKLEA & THEOHARY, *supra* note 10, Summary ("Twenty-first century criminals increasingly rely on the Internet and advanced technologies to further their criminal operations . . . . [T]hey exploit the digital world to facilitate crimes that are often technology driven, including identity theft, payment card fraud, and intellectual property theft."); *see also* Tony Bradley, *Cybercrime is the Modern-Day Mafia*, FORBES (Oct. 16, 2015, 10:38 AM), https://www.forbes.com /sites /tonybradley /2015 /10/16/cybercrime-is-the-modern-day-mafia/#6b9f778e4539 [https://perma.cc/Q9E7-S8TR].

112. *See* Wendy H. Wong & Peter A. Brown, *E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One*, 11 PERSP. ON POL. 1015, 1015 (2013) (describing "a new kind of political actor" who "engage[s] in the politics of no one via anonymizing Internet technologies" by means of hacking systems, stealing data, and disrupting systems).

VII. TATTOO SURVEILLANCE AND THE THREAT TO THE CIVIL PRESERVE

Take, for example, tattoos. Tattoos are a widespread, ancient medium of human expression that dates back at least 5,000 years.[113] By one estimate, between seven and twenty million Americans have tattoos.[114] They can signal all manners of identity—frivolous, amorous, ironic, artistic, sacred, patriotic, political, memorial, associational, ascriptive, dissenting, nonconformist, racist, or criminal.

Law enforcement has a number of legitimate interests in tattoos. Tattoos can play a critical role in witness identification.[115] Tattoos are also an integral part of law enforcement's anti-gang tactics.[116] Gang-identification training based on tattoo analysis helps to identify threats to the safety of inmates, officers, and staff of correctional facilities.[117]

The Federal Bureau of Investigation has engaged the National Institute for Standards and Technology (NIST) to

---

113. *See* Christina Smith, 21st Century Tattoo Identification and Information Sharing Thesis 5 (Jan. 5, 2015) (unpublished M.S. thesis, Bridgewater State University) (on file with the College of Graduate Studies, Bridgewater State University).

114. George B. Palermo, *The Skin and Freedom of Speech*, 55 INT'L J. OFFENDER THERAPY & COMP. CRIMINOLOGY 507, 507-508 (2011).

115. *See, e.g.*, State v. Gallegos, 853 P.2d 160, 161 (N.M. Ct. App. 1993) (holding that it was an error for the trial court to exclude a photo array of the defendant's brother's tattoos as part of his defense of mistaken identification); Commonwealth v. Crork, 966 A.2d 585, 586 (Pa. Super. Ct. 2009) (noting that a witness identified a suspect based on a single photo of the defendant's tattoo—the same tattoo the witness' saw on the robber's arm); *see also* HU HAN & ANIL K. JAIN, TATTOO BASED IDENTIFICATION: SKETCH TO IMAGE MATCHING 1-2 (2013) (citation omitted) (noting that tattoos' use in law enforcement agencies has grown due to their "prevalence among the criminal section of the population and their saliency in visual attention").

116. *See* JOHN ANDERSON ET AL., U.S. DEP'T OF JUSTICE, GANG PROSECUTION MANUAL 5 (2009) ("[G]ang unit investigators (experts) must have hands-on street knowledge of jurisdictional gangs and must develop and maintain up-to-date gang records in the form of field interview cards, police reports, probation and parole records, court adjudications of prosecutorial efforts, and *cataloged photographs of* gang members, *tattoos*, and graffiti." (emphasis added)); *see also id*. at 9 (recommending that gang files should "include photos of gang graffiti and its location; examples of various names and symbols used to identify the gang; [and] *photos of the various tattoos worn by individual members affiliated with the gang*" (emphasis added)).

117. *See* Thomas R. Zackasee, Prison Gang Tattoo Recognition: A Correctional Officer's Survival Guide 1 (Dec. 2004) (unpublished M.S. thesis, Youngstown State University), http:// docshare04 .docshare. tips /files /6289 /62890056 .pdf [https://perma.cc/EM5X-T5PT]'.

develop sophisticated tattoo-recognition technology.[118] Like other biometric technology,[119] law enforcement and counterterrorism officials will be able to identify people based on physical characteristics of tattoos.[120] Similarly, by using other mobile scanning technologies,[121] the government will be able to integrate tattoo scanners with car mounts, pole cameras, drone cameras, and body cameras.[122]

According to the Electronic Frontier Foundation, the project seeks to go beyond use of tattoos as an identifying feature to also "map connections between people with similarly themed tattoos or make inferences about people from their tattoos (e.g. political ideology, religious beliefs)."[123] On one hand, such analysis assists in identifying gang affiliations. On the other hand, such analysis is vulnerable to false positives, racial profiling, and stereotyping.

A government analysis of political ideology or religious beliefs of people bearing tattoos should give significant pause, even at a particularized, retail level. However, a proliferation of

---

118. Aaron Mackey & Dave Maass, *Tattoo Recognition Research Threatens Free Speech and Privacy*, ELECTRONIC FRONTIER FOUND. (June 2, 2016), https://www.eff.org/deeplinks/2016/06/tattoo-recognition-research-threatens-free-speech-and-privacy [https://perma.cc/5GTJ-6VEW].

119. Other examples include facial recognition, digital fingerprinting, and iris scans. *See id*.

120. *Id*.

121. *See* ELSAG, 5 INDISPENSABLE WAYS AN ALPR SYSTEM REDUCES VEHICLE-RELATED CRIMES (2017), https://cdn2.hubspot.net /hubfs /2464672 /gated-downloads /5_Indispensable_Ways.pdf— [https://perma.cc/QHR5-343Z]. Law enforcement agencies commonly use these readers for traffic and parking management, tollbooth operations, access control, and criminal investigations. *See id*. "ALPR cameras can capture up to 900 plates per minute . . . ." *Id*. Some proposed uses have generated public outcry. *See, e.g.*, Dash Coleman, *Tybee Island Abandons License Plate Scanner Plans*, SAVANNAH MORNING NEWS (Dec. 3, 2013, 1:43 PM), http://savannahnow.com /news/2013-12-02/tybee-island-abandons-license-plate-scanner-plans [https://perma.cc/G5XU-GZC3]. However, they are widely used and have been highly productive. *See* Mike Blake, *New Police Tech Has Cops Scanning License Plates to Trace Criminals*, REUTERS, June 27, 2015, https:// www.rt.com /usa / 270055- police- license- plate -scanning-criminals/ [https://perma.cc/W6KD-BS24] (noting that over a two-month period, Denver police analyzed 835,000 license-plate images leading to 17,000 hits for warrants, stolen vehicles, and other investigative leads).

122. The proliferation of these modes of camera surveillance threatens the civil preserve. *See, e.g.*, M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 29 (2011) (describing drones' threat to privacy as "just the visceral jolt society needs to drag privacy law into the twenty-first century"); Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 397, 399 (2016) (discussing privacy issues related to vantage points of police body cameras that includes victims, witnesses, suspects, and private enclaves).

123. Mackey & Maass, *supra* note 118.

mobile and stationary tattoo readers could quickly become a wholesale exercise. Big Data, government public surveillance, image storage, and algorithmic classification of tattooed people all implicate the civil preserve.[124] However, existing constitutional law likely provides no regulation of a tattoo-recognition program.

Tattoos are publicly visible to the extent not covered by clothing. Under traditional Fourth Amendment analysis, people would not have a reasonable expectation of privacy in tattoos visible to the public.[125] No individual collection by the officer or camera's observation of that which the person exposed to the public would constitute a "search" under *Katz*. Presuming tattoo scanners deployed on car mounts, poles, and officers are in public places, or capture images in plain view scenarios, the government would not engage in any *physical* intrusion that would trigger the trespass rationale established in *Jones*. In effect, a tattoo-recognition program would not be subjected to any meaningful Fourth Amendment regulation.

Two less established Fourth Amendment theories could potentially capture a challenge to a Big Data tattoo-recognition program. First, a mosaic theory approach to reasonableness could potentially establish constitutional limits on tattoo recognition. Second, there have been some cases in which the courts have suggested that technologies that transcend human sensory capacity may constitute a "search" where human vision, hearing, or smell might not. For example, in *Kyllo v. United States*,[126] the Court held that thermal imaging technology used to assess the heat in a private home constitutes a Fourth Amendment search, notwithstanding Justice Stevens's dissenting observation that "ordinary use of the senses might enable a neighbor or passerby to notice the heat emanating from [the] building."[127] Similar logic

---

124. Algorithms may perpetuate discriminatory patterns embedded in a historical dataset, and the inferential logic in their code may create new disparities that offend values of equal protection, religious freedom, or free expression. *See* Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023, 1036 (2017). Poorly designed algorithms may generate faulty data-based inferences of guilt that lead to adverse consequences. *See* Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1759 (2015) ("Big data programs may facilitate a presumption of guilt . . . ."

125. Katz v. United States, 389 U.S. 347, 351 (1967) (citing Lewis v. United States, 385 U.S. 206, 210 (1966)); United States v. Lee, 274 U.S. 559, 563 (1927)).

126. 533 U.S. 27 (2001).

127. *Id*. at 43 (Stevens, J., dissenting).

informed the analysis in *Jones* and the holding that GPS tracking of a vehicle on a public roadway that could have been surveilled by a human team nonetheless constituted a search.[128] If the Court emphasized the inhumanness of Big Data analysis in determining the reach of the Fourth Amendment, its doctrine might expand to reach cybersurveillance efforts like a tattoo-recognition program.

I am quite comfortable with the existence of a civil preserve that is presupposed by the American system. I am also comfortable with the notion that it is a constitutional value that should enjoy constitutional protections. At present, however, I am not comfortable with a translation of those two premises into constitutional legal doctrine or practice without a set of standards that lend themselves to principled application. The concepts are too amorphous for judicial operation and therefore too susceptible to judicial overreach. Therefore, there is more work to be done to establish the contours and limits of the civil preserve in any effort to establish workable constitutional safeguards to protect it. For the time being, we are left to apply existing constitutional law and seek to pass legislation addressing the unique threats posed to the civil preserve by the technological revolution.

VIII. CONCLUSION

In sum, this is an essay about stakes. A surveilled public is a chilled public. Its independence from government and the market becomes compromised with each collection. Civil society theory explains why government cybersurveillance in the Digital Age presents profound challenges to the system.

We are going to see more and more situations in which courts and policy makers struggle to apply constitutional principles across technological platforms—Xfinity, Netflix, FitBit, OnStar, Garmin, Apple Watch, Rite Aid Wellness Plus, and the Internet of Things—that interact with our daily personal lives. These thorny cybersurveillance issues will cut across traditional criminal investigations as well as counterterrorism investigations. Preservation of civil society must be the lodestar in delimiting modern cybersurveillance.

128. United States v. Jones, 565 U.S. 400, 404 (2012).