Winter 2014

Anonymity, Faceprints, and the Constitution

Kimberly L. Wehle
University of Baltimore School of Law, kwehle@ubalt.edu

ANONYMITY, FACEPRINTS, AND THE CONSTITUTION

Kimberly N. Brown[*]

INTRODUCTION

Rapid technological advancement has dramatically expanded the warrantless powers of government to obtain information about individual citizens directly from the private domain. Biometrics technology[1]—such as voice recognition, hand measurement, iris and retinal imaging, and facial recognition technology ("FRT")—offers enormous potential for law enforcement and national security. But it comes at a cost. Although much of the American public is complacent with government monitoring for security reasons,[2] people also expect to go about daily life in relative obscurity—unidentifiable to others they do not already know, do not care to know, or are not required to know—so long as they abide by the law. The reality is quite different. The government and the private sector have the capacity for surveillance of nearly everyone in America. As one commentator puts it, "soon there really will be nowhere to run and nowhere to hide, short of living in a cave, far removed from technology."[3]

FRT is a major contributor to the spectre of an Orwellian society.[4] Facebook uses it to identify "friends" from uploaded photos, which are permanently affixed in cyberspace[5] and accessible to the government.[6] Federal

---

* Associate Professor of Law, University of Baltimore School of Law. B.A., Cornell; J.D., University of Michigan. Thanks to Garrett Epps, Michele Gilman, Steve Grossman, Dave Jaros, Dionne Koller, C.J. Peters, and Colin Starger for comments on prior versions of this Article, and to Jillian Bokey, Andrew Geraghty, and Ben Bor for research assistance.

1 The field of biometrics encompasses numerous methodologies for identifying humans by their biological or behavioral characteristics or traits. *See Biometrics*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/biometrics (last visited Nov. 16, 2013).

2 Dana Blanton, *Fox News Poll: Mixed Views on NSA Surveillance Program*, FOXNEWS.COM (June 25, 2013), http://www.foxnews.com/politics/2013/06/25/fox-news-poll-mixed-views-on-nsa-surveillance-program/.

3 John W. Whitehead, *Smile, the Government Is Watching: Next Generation Identification*, RIGHT SIDE NEWS (Sept. 17, 2012, 12:07 PM), http://www.rightsidenews.com/2012091717049/editorial/us-opinion-and-editorial/smile-the-government-is-watching-next-generation-identification.html.

4 *See* GEORGE ORWELL, 1984, at 5, 169-70 (New Am. Library 1983) (1949).

5 Whitehead, *supra* note 3.

6 *See* James Risen, *Report Indicates More Extensive Cooperation by Microsoft on Surveillance*, N.Y. TIMES (July 11, 2013), http://www.nytimes.com/2013/07/12/us/report-indicates-more-extensive-cooperation-by-microsoft-on-surveillance.html (reporting on internal NSA documents indicating that "Microsoft had helped the security agency find ways to circumvent its encryption on its Outlook.com

and state authorities have their own databases of images collected from drivers' licenses, public surveillance cameras, unmanned aerial drones, and tiny recording devices attached to police uniforms.[7] Currently, the FBI is working on a $1 billion effort to expand its fingerprint identification system to cross-reference FRT and other biometric data against a vast data repository that includes some 13 million criminal mug shot photos.[8] With FRT, a federal agent or corporate marketer can convert any number of these facial images into algorithms, associate them with countless other bits of personal data accumulating throughout the global information network, and track the most intimate details of an unsuspecting person's daily life.

There is no recognized constitutional theory for placing boundaries on the government's ability to engage in ubiquitous monitoring of citizens based on images snapped in public or posted online. The Supreme Court has made clear that the Fourth Amendment does not protect "[w]hat a person knowingly exposes to the public."[9] Nor does it cover information revealed to third parties.[10] Thus, although corporations and individual citizens generate the largest storehouses of personal data today, the government—through its subpoena powers, contractual agreements, and public access to online data—can effectively bootstrap private information into its own domain without contending with the Constitution.

As a consequence, technology has minimized the Constitution's importance as a mechanism for protecting against arbitrary government tracking of one's movements, habits, relationships, interests, and thoughts. This Article attempts to reassert the Constitution's relevance when it comes to surveillance through FRT and related technologies in two ways. First, it argues for recognition of anonymity as a constitutional value that is both implicit in the Court's Fourth Amendment jurisprudence and explicit in its First Amendment jurisprudence. Second, it suggests that a shift in technology's intersection with data—from analysis of static bits of information in the pre-digital age to a "growing respect for correlations" among data in the digital age—warrants a fresh look at Fourth Amendment doctrine that ex-

---

portal's encrypted Web chat function," given the agency "access to e-mail," and "provided the F.B.I. with access to its SkyDrive service").

7 Whitehead, *supra* note 3 (discussing surveillance drones and noting that "[p]olice departments across the country are now being equipped with the Mobile Offender Recognition and Information System, or MORIS, a physical iPhone add-on that allows officers patrolling the streets to scan the irises and faces of individuals and match them against government databases"); *see also* JAY STANLEY & CATHERINE CRUMP, AM. CIVIL LIBERTIES UNION, PROTECTING PRIVACY FROM AERIAL SURVEILLANCE: RECOMMENDATIONS FOR GOVERNMENT USE OF DRONE AIRCRAFT 6-8 (2011), *available at* http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf; Carol Cratty, *FBI Uses Drones for Surveillance in U.S.*, CNN.COM (June 20, 2013, 7:27 AM), http://www.cnn.com/2013/06/19/politics/fbi-drones.

8 Whitehead, *supra* note 3.

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

10 United States v. Miller, 425 U.S. 435, 443 (1976).

cuses surveillance based on information obtained in public or from third parties.[11] FRT allows users to correlate numerical faceprint algorithms with other data points to create *new* information relating to an individual's past, present, and future life.[12] Constitutional law must account for this modern capacity to manipulate data for predictive intelligence. To this end, the Article derives doctrinal guidelines for grappling with technology's threat to the constitutional value of anonymity from a reconciliation of the Fourth and First Amendment law bearing on the issue.

Part I defines anonymity and explains that respect for the capacity to remain physically and psychologically unknown to the government traces back to the Founding. With the advent and expansion of new technologies such as FRT, the ability to remain anonymous has eroded, leading to a litany of possible harms.

Part II reviews the existing Fourth and First Amendment doctrine that is available to stave off ubiquitous government surveillance and identifies anonymity as a constitutional value that warrants more explicit doctrinal protection. Although the Fourth Amendment has been construed to excise surveillance of public and third-party information from its scope, the Court's recent jurisprudence indicates a growing recognition that constitutional doctrine is out of step with modern surveillance technologies. The Supreme Court has expressly recognized a First Amendment right to anonymous speech, which should be taken into account in assessing the constitutionality of government surveillance systems under the Fourth Amendment. This Part accordingly draws a distinction between cases that arose in the pre-digital age, in which content was often collected through physical trespass or eavesdropping, and those arising in the digital age, in which correlations among disparate points of "big data" are used to make predictions.

Part III argues that Fourth and First Amendment doctrine should be reconciled to address the manipulation—versus acquisition—of FRT data to derive new information about individuals which is exceedingly intimate and otherwise out of the government's reach. This Part suggests that this qualitative shift in information gathering is constitutionally significant under existing doctrine. Part III also offers guidelines gleaned from the intersection of First and Fourth Amendment jurisprudence for consideration by lower courts and legislators as they address the threat of limitless surveillance which big data and new technologies present.

---

[11] VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 19 (2013).

[12] *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 323 (2008).

I. THE PUBLIC VALUE OF ANONYMITY

In 1964, a commentator observed that one day "automated society [might] look upon privacy with the same air of amused nostalgia we now reserve for, say, elaborate eighteenth-century drawing room manners."[13] Numerous modern scholars have similarly declared that privacy "is in 'peril,' 'distress,' or 'danger.'"[14] Much has been written about the need to adapt Fourth Amendment law to accommodate modern infringements on privacy interests.[15] As this Part explains, FRT focuses particular attention on one aspect of privacy—the ability to manage and retain one's anonymity. This Part defines anonymity and attempts to place it in some historical context. Although American colonists lived under the constant gaze of their communities, they abhorred the officious prying of British authorities. They also robustly engaged in anonymous speech. This Part goes on to describe modern-day FRT and the threat it poses to privacy in the twenty-first century. In short, technology has put in jeopardy a value that most Americans take for granted—the ability to carry on largely incognito, if we so choose.

A. *Anonymity Defined*

Privacy is a vague notion that means different things to different people in various contexts.[16] Scholars have painstakingly developed taxonomies for privacy, parsing its subcomponents in an effort to develop a more accurate vocabulary for debate and analysis.[17] Two conceptions of privacy are particularly accessible to most laypeople.[18] Informational privacy is the

---

[13] MYRON BRENTON, THE PRIVACY INVADERS 225 (1964). Justice Brandeis observed in his *Olmstead* dissent that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court." Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting), *overruled in part by Katz*, 389 U.S. 347.

[14] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 5 (2008).

[15] *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 802-04 & n.7 (2004) (noting that "[t]he view that the Fourth Amendment should be interpreted broadly in response to technological change has been embraced by leading theorists of law and technology" and citing numerous law review articles regarding the same).

[16] Alessandro Acquisti, *Privacy and Security of Personal Information: Economic Incentives and Technological Solutions*, *in* THE ECONOMICS OF INFORMATION SECURITY 179 (L. Jean Camp & Stephen Lewis eds., 2004); *see generally* SOLOVE, *supra* note 14, at ix, 1 ("There is no overarching conception of privacy—it must be mapped like terrain, by painstakingly studying the landscape. . . . Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.").

[17] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 483-84 (2006).

[18] Professor Anita Allen distinguishes the two primary usages of the term "privacy" as, on the one hand, "conditions of restricted access," including anonymity, physical separation or isolation from

interest in "avoiding disclosure of personal matters" and controlling one's own personal information, which the Supreme Court has suggested is constitutionally protected when gathered and held by the government.[19] Today, the term often relates to information stored on computer systems, such as medical records, financial data, criminal records, political records, business-related information, and online data.[20] Physical privacy has traditionally been equated with the protection of one's person or physical space, such as a home or vehicle. Violations of physical privacy can trigger Fourth Amendment and/or common law scrutiny.[21] People intrinsically appreciate the need for legal limits on the ability of the government and others to invade one's home or body absent consent.

Related to both informational and physical privacy—but less salient in the collective mind of the public—is the concept of anonymity: the state of hiding in plain sight from the government so long as one abides by the rule of law. Anonymity is the freedom from being identified and tracked by name while going through the motions of daily life, including physical movement in private and public spaces, the transaction of business online, and the maintenance of personal and professional relationships, habits, and beliefs—however unpopular or repugnant.[22] Anonymity enables one to re-

---

others, and information nondisclosure, and, on the other hand, privacy as liberty—that is, "freedom from governmental or other outside interference with decisionmaking and conduct, especially respecting appropriately private affairs." Anita L. Allen, *Taking Liberties: Privacy, Private Choice, and Social Contract Theory*, 56 U. CIN. L. REV. 461, 464-66 (1987) (footnotes omitted); *cf.* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2092 (2001) (discussing privacy as control of knowledge, a protector of dignity—which is most relevant to the Fourth Amendment—and a means of implementing freedom). In this Article, only the restricted access form of privacy is at issue under Professor Allen's rubric.

[19] *See* NASA v. Nelson, 131 S. Ct. 746, 751 (2011) ("We assume, without deciding, that the Constitution protects [such] a privacy right . . . ."); Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977) (characterizing such interest as "[o]ne element of privacy"); Whalen v. Roe, 429 U.S. 589, 599-600 (1977) (noting that the Court's privacy cases have implicated "the individual interest in avoiding disclosure of personal matters" as well as "the interest in independence in making certain kinds of important decisions").

[20] Scholars have divided data collection into subcategories, including "tool data," which encompasses data—such as social security numbers and dates of birth—that is valued for its utility versus its content; "biographical data," which is "the product of . . . behavior in public places" and includes residence, routines, and friends; and "transactional data," which is information generated by interactions with professionals such as doctors, accountants, and lawyers, as well as vendors of goods and services. Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 54 n.247 (2005) (citing sources).

[21] A third foundational prong of privacy is decisional privacy, or the right to make fundamental decisions—such as the use of contraception methods—without governmental interference. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

[22] Anonymity is a conception of privacy which may be captured in the literature under different names. *Cf.* SOLOVE, *supra* note 14, at ix, 1 (identifying freedom from surveillance as a concept embraced by the term).

main undifferentiated in public. In literal terms, it means "nameless."[23] As Justice Sotomayor suggested in *United States v. Jones*,[24] the everyday occurrences for which anonymity is appreciated "take[] 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."[25] In protecting against government access to one's physical whereabouts, anonymity shelters private information about one's thoughts, relationships, and plans for the future.[26] It fosters the capacity to control or limit access to "one's intimate relationships or aspects of life"[27] and, accordingly, to exclude others from the very "consciousness of the mind."[28]

In the late eighteenth century, philosopher Jeremy Bentham famously unveiled his "panopticon" design for institutional buildings, which contained a central tower surrounded by a perimeter of backlit cells from which inmates could not see their surveyors.[29] Bentham described the design as "[a] new mode of obtaining power of mind over mind," as a single guard could theoretically control all of the prisoners simultaneously.[30] As French philosopher Michel Foucault later explained, the prisoners would internalize the presumption that they are being watched and modify their behavior to comply with expectations,[31] rendering the guards virtually superfluous. Legal theorists who have studied the panopticon effect posit that "[a]nonymity in public promotes freedom of action and an open society," while a "[l]ack of public anonymity promotes conformity and an oppressive

---

23 Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 238 (2002).

24 132 S. Ct. 945 (2012).

25 *Id.* at 955 (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)) (internal quotation marks omitted).

26 Taken to the extreme, true autonomy is the ability to hide from others without a trace. It has some positive value, such as in the situation where government informants assume a new identity for their own protection. It is also problematic to the extent that it enables wrongdoers to evade responsibility for their actions. *See generally* Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1641-43 (1995). In the online environment, "[a]nonymity can be used to violate another's privacy." *Id.* at 1661 (quoting Posting of L. Detweiler, ld231782@longs.lance.colostate.edu, to alt.privacy et al. (Sept. 20, 1993), *available at* http://www.websteruniv.edu/~bumbaugh/net/net-anon.pt2).

27 SOLOVE, *supra* note 14, at 13.

28 Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 268 (1977).

29 JEREMY BENTHAM, THE PANOPTICON WRITINGS 35 (Miran Bozovic ed., 1995).

30 *Id.* at 31.

31 *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 195, 201 (Alan Sheridan trans., 2d ed. 1995) (1977).

society"[32] in which "majoritarian authority will coerce citizens into silence or acquiescence."[33]

Although Bentham never built his panopticon, the association of privacy with anonymity from the government later appeared in the writings of Samuel Warren and Louis Brandeis, who in 1890 recognized "the right to be let alone"[34] as an important definitional component of privacy and one that has since become "the foundation of privacy law in the United States."[35] In the twentieth century, Professor William Prosser similarly identified intrusions upon a person's seclusion or solitude as a distinct kind of privacy invasion against which the law should provide protection.[36]

Social science research suggests that contemporary Americans view the ability to move about in public or online without being tracked as an important aspect of privacy.[37] Surveys indicate that Internet users perceive an invasion of privacy when their web-surfing information is collected and shared with other parties.[38] People especially want to maintain a meaningful degree of independence from the government when it comes to personal thoughts and communications with others. Even before online technology took hold, survey respondents ranked the monitoring of phone calls for thirty days and the reading of a personal diary as more intrusive than the government's withdrawal of blood.[39] An area of particular public concern is video surveillance, which may arouse fears of rigid and arbitrary law en-

---

32 Slobogin, *supra* note 23, at 240.

33 Jonathan Turley, *Registering Publius: The Supreme Court and the Right to Anonymity*, CATO SUP. CT. REV. 2001-2002, at 57, 75-76, 82. Jonathan Turley has identified six additional benefits of anonymity in the area of free speech: (1) protecting against persecution for unpopular speech; (2) preventing disenfranchisement from public debate and participatory politics; (3) encouraging pluralistic value and thoughts; (4) protecting spontaneous speech which "is the type of speech that occurs between neighbors"; (5) enhancing privacy values by enabling people "to separate their personal home life from their public advocacy"; and (6) protecting Internet speech, in particular, as the looming "threat of government surveillance" makes the Internet a rare site of anonymous discourse that can "remain[] raw and uninhibited." *Id.* at 75-78; *see also id.* at 77, 83 (noting that loss of anonymity signifies a loss of freedom).

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

35 SOLOVE, *supra* note 14, at 15. The right to be left alone has been critiqued as too broad in and of itself. *Id.* at 18. "If privacy simply meant 'being let alone,' . . . [a] punch in the nose would be a privacy invasion as much as a peep in the bedroom." *Id.* (quoting ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 7 (1988)) (internal quotation marks omitted).

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

37 LISA S. NELSON, AMERICA IDENTIFIED: BIOMETRIC TECHNOLOGY AND SOCIETY 94-97 (2011); *see also* Slobogin, *supra* note 23, at 273-86 (discussing earlier poll data on surveillance).

38 Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 622-29 (2011).

39 Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 737-39 (1993).

forcement by an omniscient state.[40] National surveys and focus groups indicate that "the threat of misuse of biometric identifiers [is] a point of concern and an obstacle to social acceptance" of such technologies.[41] This attitude is reflected in survey participants' relative distaste for the use of biometric identification systems in public events like a professional football game, which was "viewed as a transgression of anonymity and decisional autonomy without sufficient policy justification or assurance that the identification could be carried out with accuracy and reliability."[42]

People appear to be more willing to tolerate privacy intrusions where the government's use of their personal information would foster their own well-being.[43] The cost-benefit calculus imperceptibly performed around the acceptability of new technology, moreover, can be affected by the perceived urgency of its public safety benefits. In the months after 9/11, 51 percent of people surveyed expressed greater trust in government than survey respondents did a year earlier.[44] Respondents were also more comfortable with decreased anonymity when biometric technology was used for boarding a plane, accessing government buildings, checking against a terrorist watch list, or requiring background checks on foreigners.[45] In a CBS/New York Times poll taken after the Boston Marathon attacks, 78 percent of respondents endorsed the idea of having more public surveillance cameras such as those that helped identify the bombing suspects; only 20 percent said that the government has gone too far in restricting civil liberties in the battle against terrorism.[46]

Anonymity is nonetheless something that Americans generally take for granted. People expect to be able to recede into a crowd or go unnoticed while walking down the street so long as they have nothing illegal to hide. At this juncture, there is "insufficient public awareness" about FRT, as well as "zero auditing mechanisms in place for any entity using the technologies."[47] As a consequence, the public is unable to meaningfully perform a cost-benefit calculus regarding the government's use of new technologies for various forms of surveillance. They can only react when employment of

---

40 Andrew W. Senior & Sharathchandra Pankanti, *Privacy Protection and Face Recognition*, *in* HANDBOOK OF FACE RECOGNITION 671, 672 (Stan Z. Li & Anil K. Jain eds., 2d ed. 2011).

41 NELSON, *supra* note 37, at 174.

42 *Id.* at 118.

43 *See id.* at 158.

44 *Id.* at 157 (citing Robert Putnam, *Bowling Together*, AM. PROSPECT (Jan. 18, 2002), http://prospect.org/article/bowling-together-0).

45 *Id.* at 114-17.

46 Rob Quinn, *Poll: 78% Now OK with More Surveillance Cameras*, NEWSER.COM (May 1, 2013), http://www.newser.com/story/167141/poll-78-now-ok-with-more-surveillance-cameras.html.

47 Violet Blue, *Why You Should Be Worried About Facial-Recognition Technology*, CNET.COM (Aug. 29, 2012, 1:58 PM), http://news.cnet.com/8301-1023_3-57502284-93/why-you-should-be-worried-about-facial-recognition-technology/ (citing remarks by Privacy Rights Clearinghouse Director Beth Givens).

state-of-the-art surveillance methods makes headlines. In a separate CNN/Time poll taken two weeks after the Boston tragedy, 61 percent of respondents were more concerned about government expansion of anti-terrorism policies that restrict civil liberties than they were about the government failing to enact new policies to fight terrorism.[48] As information technology continues to gain in intelligence and efficiency, it becomes increasingly difficult for individuals to emerge from anonymity, engage in a non-anonymous transaction (such as withdrawing money from an ATM machine), and then return to anonymity. We live in an age in which people care deeply about privacy yet routinely provide information online in exchange for some perceived benefit,[49] such as the ease of making a purchase transaction, or the social or professional networking that social media provides. Young people who have grown up with technology might not even conceive of a personal photo as private at all.[50] What many Americans fail to appreciate is that technology has put society on a trajectory whereby, even if the interiors of homes and bodies are kept private, and even if the law continues to protect against disclosures of certain categories of personal information, anonymity will soon become a relic of history.[51]

B. *Anonymity Historically*

Personal privacy was hard to come by in colonial America.[52] Colonial travelers shared beds with strangers due to the "practical necessity" of the "warmth and protection of a small group."[53] The lack of ceilings in early homes enabled gawking from the roof beams.[54] Individuals were perceived primarily as part of a family or community, which collectively monitored

---

48 Zeke J Miller, *Poll: Americans More Concerned About Civil Liberties in Wake of Boston Bombing*, TIME (May 1, 2013), http://swampland.time.com/2013/05/01/poll-americans-more-concerned-about-civil-liberties-in-wake-of-boston-bombing/.

49 SOLOVE, *supra* note 14, at 5.

50 Anecdotally, when asked about privacy and the Internet, "[law] students argued strongly in favor of a right to anonymity." Turley, *supra* note 38, at 75.

51 JONATHAN FRANZEN, *Imperial Bedroom*, *in* HOW TO BE ALONE 39, 40 (2003) (observing that what is missing in the modern discussion of privacy and technology is "a genuinely alarmed public").

52 Brenner, *supra* note 20, at 41 (citing ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 17, 19 (2000)).

53 DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 76 (1972).

54 Brenner, *supra* note 20, at 41 (citing SMITH, *supra* note 52, at 19-20). "Even husbands and wives sometimes shared their bedrooms with lodgers or other members of the family." FLAHERTY, *supra* note 53, at 77. One woman who shared a bed with an unmarried couple later testified that "[t]he Bed was very Narrow on which they three were and thinks it almost if not wholly impossible that they should be guilty of that Crime [intercourse] without her knowledge and She observed no such thing." *Id.* (internal quotation marks omitted).

members' habits and exerted pressure to conform.[55] Newcomers to New England towns needed permission to settle there,[56] and residents were required to register the names of overnight guests.[57] Colonial laws forbade residents from living alone or far from "the meeting house," or center of town, as was the practice in England.[58] Court records show that Massachusetts homes were systematically searched in 1668 for single persons to be relocated with families.[59] Opposition to solitary living "was motivated, not by lack of concern for privacy, but by traditions, practicality, and an underlying fear of sin."[60] From the perspective of the church, living together as a family unit was the best arrangement for individuals and the community as a whole.[61] By the eighteenth century, however, "New England society was prepared to accept the person who wanted to live alone because he enjoyed the privacy this way of living provided."[62]

While living conditions afforded colonists little privacy, the pre-technological world enabled greater privacy relative to the present day in other respects. Inevitably, reputational information was circulated as people moved about,[63] but people could avoid eavesdropping by conducting conversations beyond the earshot of others.[64] Business was transacted with scant written exchanges,[65] and personal records consisted largely of diaries or letters.[66] Only one person possessed a paper at any given time, and copies

---

55 Brenner, *supra* note 20, at 40-41 (quoting GINI GRAHAM SCOTT, MIND YOUR OWN BUSINESS: THE BATTLE FOR PERSONAL PRIVACY 24 (1995)).

56 FLAHERTY, *supra* note 53, at 170. Connecticut law from 1636 read that "no man that is neither married, nor hath any servant, nor is a publick Officer shall keep house of himself without consent of the Town where he lives." ANDREW J. CHERLIN, THE MARRIAGE-GO-ROUND: THE STATE OF MARRIAGE AND THE FAMILY IN AMERICA TODAY 41 (2009) (internal quotation marks omitted).

57 SMITH, *supra* note 52, at 10.

58 Brenner, *supra* note 20, at 41.

59 SMITH, *supra* note 52, at 10; *see also* CHERLIN, *supra* note 56, at 41 (explaining, in the verbiage of the times, that selectmen of a Massachusetts town met in the 1670s "to setel the younge persons in such families in the Town as is most sutable for thier good" (internal quotation marks omitted)).

60 FLAHERTY, *supra* note 53, at 175; *see also* CHERLIN, *supra* note 56, at 41 ("In part, these laws reflected the reality that living alone was nearly impossible in an environment where people needed family members to help them obtain the food, clothing, and shelter they needed to survive.").

61 SMITH, *supra* note 52, at 10.

62 FLAHERTY, *supra* note 53, at 179 ("The residents of seventeenth-century New England regarded the desire to live alone with suspicion. Morality and the economic interests of the state were better served if everyone lived in a family. Yet this was not an expression of total hostility to the value of privacy. . . . By the latter part of that century experience in America had shown that it was possible to live alone and not become a burden on the community.").

63 Brenner, *supra* note 20, at 83.

64 FLAHERTY, *supra* note 53, at 115 ("In colonial America, of course, conversations could only occur in the physical presence of someone else.").

65 Brenner, *supra* note 20, at 82-83.

66 *Id.* at 83.

had to be painstakingly recreated.[67] Individuals could control personal documents by securing them in a desk or cabinet in their own home.

Moreover, "[d]espite the casualness of delivery, there seems to have been little premeditated and malicious perusal of other people's mail" in the seventeenth century.[68] The Post Office Act of 1710 mandated that "No Person or Persons shall presume wittingly, willingly, or knowingly, to open, detain, or delay . . . any Letter or Letters, Packet or Packets."[69] Colonists who were concerned about prying British authorities developed codes for encrypting their letters[70] and used sealing wax and wrapping paper on packages.[71] It was not until 1835 that postmasters attempted to monitor content in response to efforts by Southerners to make illegal the transmission of abolitionist literature through the mail.[72] In *Ex parte Jackson*,[73] the Supreme Court upheld a statute banning the transmission of lotteries via the mail, but noted that "[l]etters and sealed packages of this kind in the mail are as fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles."[74] Thus, when given the opportunity, the late-nineteenth-century Court upheld citizens' privacy in their personal mail.

Although colonists lived in the public eye of their communities, the Framers forbid their newly formed American government from searching a person's private papers without first obtaining a warrant,[75] a requirement that dates back to the English common law.[76] Whereas specific warrant provisions were included in even the earliest state constitutions,[77] the Fourth

---

67 *Id.* (citing WALTER BESANT, LONDON IN THE TIME OF THE STUARTS 53 (1903)) (describing seizure of the "papers" of James Howell, who was a suspected spy).

68 FLAHERTY, *supra* note 53, at 119.

69 *Id.* at 120 (quoting Post Office (Revenues) Act, 1710, 9 Ann., c. 11, § 41) (internal quotation marks omitted).

70 *See* SMITH, *supra* note 52, at 25 ("For letter writers in the Colonial period, the consequences were serious if their writings were disclosed, especially if the messages appeared to defy the Crown or to be otherwise suspicious. . . . To be safe, letter writers developed means for preserving the confidentiality of their correspondence [and] codes for disguising their words."); *see also* FLAHERTY, *supra* note 53, at 118 ("Others employed codes, shorthand, or nicknames when writing to friends, particularly on political topics.").

71 FLAHERTY, *supra* note 53, at 118.

72 Michael T. Gibson, *The Supreme Court and Freedom of Expression from 1791 to 1917*, 55 FORDHAM L. REV. 263, 294 & n.203 (1986).

73 96 U.S. 727 (1877).

74 *Id.* at 733.

75 Brenner, *supra* note 20, at 83.

76 *See* Thomas Y. Davies, *Correcting Search-and-Seizure History: Now-Forgotten Common-Law Warrantless Arrest Standards and the Original Understanding of "Due Process of Law,"* 77 MISS. L.J. 1, 8 (2007).

77 *See* Hans A. Linde, *State Constitutional Law*, in 5 ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION 2495, 2496 (Leonard W. Levy & Kenneth L. Karst eds., 2d ed. 2000) ("Constitutional entrenchment of individual rights began with the earliest state constitutions . . . and is universal

Amendment came into effect as part of the Bill of Rights in 1791.[78] The Supreme Court has deemed "the familiar history" of the Fourth Amendment as reflecting "a choice that our society should be one in which citizens 'dwell in reasonable security and freedom from surveillance.'"[79] Its "commands grew in large measure out of the colonists' . . . memories of the general warrants formerly in use in England. These writs . . . granted sweeping power to . . . agents of the King to search at large for smuggled goods."[80] Indeed, "aside from searches incident to arrest, such warrantless searches were not a large issue in colonial America."[81]

While the warrant requirement was adopted to stave off the intrusiveness of the Crown, "anonymous speech flourished" in social and political life around the time that freedom of speech and freedom of association became constitutionally protected under the First Amendment.[82] For the Founding Fathers, anonymity in the authorship of newspapers and pamphlets was central to attracting public support for the Revolution and formation of an independent government without evoking British punishment.[83] Although speech was strictly limited during the years of the Alien and Sedition Acts of 1798,[84] the laws' constitutionality was the subject of much debate at the time.[85] In a famous sedition trial in 1735, a printer refused to reveal the authors of anonymous attacks on the Crown Governor of New York, an act which, according to Justice Thomas in his concurring opinion in *McIntyre v. Ohio Elections Commission*,[86] "signified at an early moment the extent to which anonymity and the freedom of the press were intertwined in the early American mind."[87] In 1788, Alexander Hamilton, James Madison, and John Jay published "the most famous example of the outpouring of anonymous political writing that occurred during the ratifica-

---

throughout the states, though the statements of rights differ. The common tradition includes . . . freedom from warrantless and unreasonable searches and seizures . . . .").

78 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, and no Warrants shall issue, but upon probable cause . . . .").

79 California v. Ciraolo, 476 U.S. 207, 217 (1986) (Powell, J., dissenting) (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).

80 United States v. Chadwick, 433 U.S. 1, 7-8 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

81 *Id.* at 8.

82 Turley, *supra* note 33, at 61.

83 *Id.* at 58.

84 *See* Kurt T. Lash & Alicia Harrison, *Minority Report: John Marshall and the Defense of the Alien and Sedition Acts*, 68 OHIO ST. L.J. 435, 438 (2007) (describing how the Acts allowed for deportations of those considered aliens and criminalized political opposition to the government).

85 *See id.* The statutes lapsed in 1801, after which the Supreme Court declared that there was no federal jurisdiction over state law criminal charges for seditious libel. United States v. Hudson, 11 U.S. (7 Cranch) 32, 34 (1812).

86 514 U.S. 334 (1995).

87 *Id.* at 361 (Thomas, J., concurring in the judgment).

tion of the Constitution"[88]—the Federalist Papers. They used the pseudonym "Publius" to disseminate the treasured constitutional writings, and signed others as "An American Citizen," "Marcus," and "Americanus."[89]

Anonymous speech—and opposition to it—continued to play a central role in political discourse after Ratification. The Continental Congress famously attempted to identify an article by Benjamin Rush, who published his attack on members of Congress for inflation, embezzlement, and fraud under the name "Leonidas."[90] When a Massachusetts delegate moved to require the article's printer to appear before Congress and discuss Leonidas, several members successfully opposed the motion on the grounds that it violated freedom of the press.[91] Federalists and Anti-Federalists continuously sparred in essays written under fictitious names like "Caesar," "A Countryman," "Fabius," and "Landowner" on the one hand and "Cato," "Brutus," "Cincinnatus," and "Federal Farmer" on the other.[92] James Madison and Alexander Hamilton also used the famous pseudonyms "Helvidius" and "Pacificus" in debates over President Washington's decision to remain neutral in the war between the British and the French.[93] Scholars have surmised from these and other examples that "[t]he historical use of anonymous speech strongly suggests that the Framers originally viewed anonymity as a vital part of free speech and freedom of the press."[94]

In the nineteenth century, new technologies for law enforcement emerged as cities increasingly faced crime and civil disobedience stemming from population growth, ethnic and racial tensions, and economic failures.[95] With the invention of the telegraph in 1844 and the telephone in 1876, elec-

---

88 *Id.* at 360; *see generally* Gregory E. Maggs, *A Concise Guide to the Federalist Papers as a Source of the Original Meaning of the United States Constitution*, 87 B.U. L. REV. 801, 802 (2007).

89 Victoria Smith Ekstrand, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 COMM. L. & POL'Y 405, 406 (2003); *see also* Turley, *supra* note 33, at 59.

90 *McIntyre*, 514 U.S. at 361 (Thomas, J., concurring in the judgment) (citing Henry Laurens' Notes of Debate (July 3, 1779), *in* 13 LETTERS OF DELEGATES TO CONGRESS 1774-1789, at 139, 141 n.1 (Paul H. Smith et al. eds., 1986)).

91 *Id.* at 362 (citing Dwight L. Teeter, *Press Freedom and the Public Printing: Pennsylvania, 1775-83*, 45 JOURNALISM Q. 445, 451 (1968)).

92 Turley, *supra* note 33, at 59-60 & nn.11-23 (footnotes omitted) (identifying who actually used these names, where possible).

93 *McIntyre*, 514 U.S. at 369 (Thomas, J., concurring) (citing Alexander Hamilton, *Pacificus No. 1, June 29, 1793, in* 15 THE PAPERS OF ALEXANDER HAMILTON 33-43 (H. Syrett ed. 1969); James Madison, *Helvidius No. 1, Aug. 24, 1793, in* THE PAPERS OF JAMES MADISON 66-73 (Thomas A. Mason, Robert A. Rutland & Jeanne K. Sisson eds., 1985)); *see also id.* at 361-62 (Thomas, J., concurring) (providing additional examples of anonymous speech).

94 Turley, *supra* note 33, at 61.

95 Craig D. Uchida, The Development of the American Police: An Historical Overview 8 (Dec. 2004) (manuscript), *available at* http://storage.globalcitizen.net/data/topic/knowledge/uploads/2009042815114290.pdf.

tronic communication made individual surveillance much easier.[96] In 1890, Samuel Warren and Louis Brandeis bemoaned that "[i]nstantaneous photographs and newspaper enterprise [had] invaded the sacred precincts of private and domestic life."[97] With the advancement of photography, "amateurs [could] take 'candid' photographs, often clandestinely," in lieu of the prolonged professional sittings that preceded George Eastman's invention of the handheld camera in 1884, and newspapers came to thrive on "sin, sex and violence."[98] Wireless police radios,[99] polygraphs,[100] and the use of fingerprints for personal identification emerged in the late nineteenth and early twentieth centuries.[101] Law enforcement relied heavily on wiretapping to monitor social unrest caused by poor working conditions, World War I, and Prohibition.[102]

In the second half of the twentieth century, the government's technological powers for visual surveillance became more sophisticated, allowing it "to peer into homes, high rise apartments, and commercial establishments," as well as "remote private areas."[103] Night vision devices enabled long-range military surveillance,[104] and aerial mapping cameras allowed for precision topographical photography.[105] As Professor Daniel Solove has observed, it was "the profound proliferation of new information technolo-

---

96 DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 85 (2d ed. 2009); *see also* CLAUDE S. FISCHER, AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940, at 71, 225 (1992).

97 Warren & Brandeis, *supra* note 34, at 195.

98 Brenner, *supra* note 20, at 32 (citing Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1351) (internal quotation marks omitted); *see* SMITH, *supra* note 52, at 124.

99 VIKRANT VIJ, WIRELESS COMMUNICATION 1-2 (2010).

100 DENNIS C. TANNER & MATTHEW E. TANNER, FORENSIC ASPECTS OF SPEECH PATTERNS: VOICE PRINTS, SPEAKER PROFILING, LIE AND INTOXICATION DETECTION 60-61 (2004).

101 *See generally* WILLIAM J. HERSCHEL, THE ORIGIN OF FINGER-PRINTING (1916).

102 SOLOVE & SCHWARTZ, *supra* note 96, at 85; Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 508 (2013). In 1934, Congress enacted § 605 of the Federal Communications Act, which made unauthorized wiretapping a federal crime. Pub. L. No. 416, § 605, 48 Stat. 1064, 1103-04 (1934). Section 605 was amended in 1968 by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. 3, 82 Stat. 197, 211-25 (1968) (codified at 18 U.S.C. §§ 2510-20 (2006)), and again in 1986 by the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522 (2006)). Under the Wiretap Act, which is part of the ECPA, "courts can authorize continuing surveillance—24 hours a day for a 30-day period, which can be extended." DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 92 (2006).

103 Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 678-79 (1988) (footnotes omitted) (describing a positive relationship between technological advances in surveillance and intrusion on privacy).

104 *Id.* at 678 n.162.

105 *See* Dow Chem. Co. v. United States, 476 U.S. 227, 242-43 & n.4 (1986).

gies during the twentieth century—especially the rise of the computer—[that] made privacy erupt into a frontline issue around the world."[106]

In addition to using surveillance technologies, the government has long obtained personal information about individual citizens by requiring its disclosure as an obligation of citizenship. Although the modern census gathers information about race, income, and age, the first Congress rejected proposals from James Madison to require such disclosures, instead using binary categorizations such as woman or man, slave or free man, and adult or child.[107] The Department of State began issuing passports to American citizens traveling abroad in 1789.[108] Passports were mandated for international travel during the Civil War and World War I[109] and have been, as a general rule, since 1952.[110] In 1835, the Supreme Court acknowledged that "[i]t is understood, as matter of practice, that some evidence of citizenship is required, by the secretary of state, before issuing a passport."[111]

Congress instituted the first income tax in 1861 as a means of raising revenue for the Civil War.[112] The law imposed a 5-percent tax on the "annual gains, profits, or income of every person residing in the United States" for incomes exceeding six hundred dollars.[113] With the passage of the Sixteenth Amendment in 1913, the federal government gained the power to require the filing of personal financial information, such as gross income, on tax returns.[114] The first social security number was issued through the U.S. Postal Service in 1936,[115] and since then social security numbers have come to function as unique personal identifiers[116] that are routinely linked to property ownership, residence histories, medical records, and other public transactions.

The government's power to require disclosures of individual data expanded with the rise of the administrative state in the early twentieth centu-

---

106 SOLOVE, *supra* note 14, at 4.

107 Carrie Pixler, Note, *Setting the Boundaries of the Census Clause: Normative and Legal Concerns Regarding the American Community Survey*, 18 WM. & MARY BILL RTS. J. 1097, 1114 & n.118 (2010).

108 *See Passport Applications*, NAT'L ARCHIVES, http://www.archives.gov/research/passport/index.html (last visited Nov. 24, 2013) (citing Act of Aug. 18, 1856, 11 Stat. 52, 60).

109 *See id.* (citing Act of May 22, 1918, Pub. L. No. 65-154, 40 Stat. 559; Act of June 20, 1941, Pub. L. No. 77-113, 55 Stat. 252).

110 Kent v. Dulles, 357 U.S. 116, 121 (1958) (citing 8 U.S.C. § 1185).

111 Urtetiqui v. D'Arcy, 34 U.S. (9 Pet.) 692, 699 (1835).

112 LAWRENCE H. SELTZER, THE NATURE AND TAX TREATMENT OF CAPITAL GAINS AND LOSSES 31 (1951).

113 Revenue Act of 1862, 12 Stat. 432, 473.

114 U.S. CONST. amend. XVI; *see* I.R.C. § 6103(d)(1) (2006) (allowing disclosure to enforce tax laws); *id.* § 6103(h)(4)(D), (i) (authorizing disclosure by court order).

115 *The First Social Security Number and the Lowest Number*, SOC. SECURITY ADMIN., http://www.ssa.gov/history/ssn/firstcard.html (last visited Nov. 20, 2013).

116 Brenner, *supra* note 20, at 54 n.247.

ry.[117] In addition to social security information, federal agencies now maintain thousands of databases with records pertaining to immigration, bankruptcy, military history, and the receipt of federal benefits. Federal legislation governing housing assistance now enables any law enforcement officer to obtain the address, social security number, and photo of assistance recipients without formal legal process.[118] In addition, states possess "records of births, marriages, divorces, professional licenses, voting information, worker's compensation, personnel files (for public employees), [and] property ownership," as well as information about crimes, victims, and arrests.[119] Some require the collection of biometric information and random drug tests as preconditions to receiving public benefits.[120]

The government's legal authority to collect identifying data on individuals derives from a number of sources.[121] Federal agencies collect a substantial amount of information pursuant to legislation authorizing complex systems of taxation, regulation, licensing, and entitlement distribution. For law enforcement, the constitutional gold standard is probable cause and a warrant. The government may alternatively use judicial, grand jury, and administrative subpoenas and court orders, often upon a showing of mere relevance.[122] Modern governmental data collection increasingly involves the ability to obtain substantial amounts of information about private citizens without any formal process.[123] Administrative and law enforcement agencies can simply purchase personal data from private sector companies[124] or mine what already exists in the public domain.[125] Since the private sector has turned personal data collection into a multibillion-dollar industry,[126] the

---

117 SOLOVE & SCHWARTZ, *supra* note 96, at 243-44.

118 42 U.S.C. § 1437z (2006); Murphy, *supra* note 102, at 509.

119 Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002).

120 Murphy, *supra* note 102, at 510.

121 This Article does not distinguish between state and local police departments, national law enforcement agencies, and federal agencies engaged in national security functions, the last of which raise a host of different legal and policy issues that are beyond the scope of this piece.

122 Murphy, *supra* note 102, at 517-18 (citing various legislative provisions for court-ordered disclosure of otherwise private information).

123 *See generally* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013) (explaining that the gathering of computerized employment, customer, and medical records by private and public entities began in the 1960s and led to nearly fifty congressional hearings on data privacy issues); *see also infra* notes 398-401 and accompanying text (discussing *Whalen v. Roe*, 429 U.S. 589 (1977), in which the Court recognized a constitutional interest in avoiding disclosure of personal information).

124 Murphy, *supra* note 102, at 511.

125 *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 325 (2012); *see generally* Murphy, *supra* note 102, at 519-20 (discussing federal statutes governing the use of information collected by law enforcement).

126 *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY GLOBAL INST., http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_

vitality of this last method is becoming a hallmark of twenty-first century government surveillance.

Private parties have historically lacked equivalent access to others' personal information absent the use of private investigators, civil lawsuits, consent, trespass, or theft. This is in part a consequence of the enumerated constitutional and statutory powers of the federal government,[127] as well as the states' residuary "police powers," which the Supreme Court has characterized as "the time-tested conceptional limit of public encroachment upon private interests [for] 'the interests of the public.'"[128] Police powers include the authority to perform searches of persons or property, to interrogate those in custody, and to subpoena witnesses and documents in both the criminal and civil contexts.[129] Although civil discovery is broad, "this power does not begin to compare with the power of compulsion under grand jury subpoena or the intrusion incident to a physical search for documents."[130]

With the inventions of the computer and the Internet, however, the private sector's capacity for gathering massive amounts of personal data for commercial purposes has exploded. Individual private corporations in the United States have more stored data than the Library of Congress.[131] If the total information that exists globally today were transferred to CD-ROMs, "they would stretch to the moon in five separate piles."[132] The sheer glut of data has changed "the essence" of information itself.[133] "In a big-data world, . . . we won't have to be fixated on causality; instead we can discover pat-

---

the_next_frontier_for_innovation (last visited Nov. 20, 2013) ("[U]sers of services enabled by personal-location data could capture $600 billion in consumer surplus.").

127 U.S. CONST. art. II, § 1, cl. 1; *id.* § 3. The ability of the President to provide for national security, for example, is a power derived from the enumerated powers of Article II, and it often allows the Executive branch greater access to the personal information of private citizens. *See generally* HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION: SHARING POWER AFTER THE IRAN-CONTRA AFFAIR 67-72 (1990) (noting that the Constitution creates three branches of government and vests them with powers that affect foreign affairs and national security, but that because "[m]ost often, the text simply says nothing about who controls certain domains . . . [such as] the conduct of covert action," one must look to constitutional structure, statutes, and custom to understand the source of such powers).

128 Goldblatt v. Town of Hempstead, 369 U.S. 590, 594-95 (1962) (quoting Lawton v. Steele, 152 U.S. 133, 137 (1894)); *see also* United States v. Morrison, 529 U.S. 598, 618-19 (2000) (observing that the Constitution created a federal government of limited powers, while reserving a generalized police power to the states). For a discussion of the origins and meaning of the term, see Santiago Legarre, *The Historical Background of the Police Power*, 9 U. PA. J. CONST. L. 745 (2007).

129 Kenneth Mann, *Punitive Civil Sanctions: The Middleground Between Criminal and Civil Law*, 101 YALE L.J. 1795, 1810-11 (1992).

130 *Id.* at 1811 n.56.

131 MAYER-SCHÖNBERGER & CUKIER, *supra* note 11, at 8; *see* JAMES MANYIKA ET AL., MCKINSEY GLOBAL INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 19 (2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation (click "Full Report" hyperlink).

132 MAYER-SCHÖNBERGER & CUKIER, *supra* note 11, at 9.

133 *See id.* at 9-10.

terns and correlations in the data that offer us novel and invaluable insights."[134] By applying a mathematical algorithm to hundreds of billions of searches, for example, Google can identify a disease outbreak with stunning accuracy.[135] Online retailers such as Amazon.com routinely make real-time merchandise suggestions from browsing and purchase data.[136] Information on social networking sites enables companies to identify when, how, and by whom their products are being discussed.[137] Web bug trackers allow "[a]nalytics and ad serving companies [to] track user behavior across large portions of the web."[138]

The government now mines huge amounts of personal data from online private sector companies without first obtaining a search warrant, subpoena, court order, or consent.[139] Although police investigations have always involved information collection, the amount and variety of data involved today—and the technological ability to create new information by cross-referencing data points with other data points—is new.[140] By drawing

---

134 *Id.* at 14.

135 *Id.* at 11.

136 Douglas Page, *Crime Fighting's Next Big Deal*, OFFICER.COM (Sept. 4, 2012), http://www.officer.com/article/10773317/crime-fightings-next-big-deal.

137 J. D. Heyes, *NSA Social Spy Network Facebook to Use Facial Recognition Technology to Track Individuals Across Photos, Videos*, PRISON PLANET (June 24, 2012, 5:52 AM), http://www.prisonplanet.com/nsa-social-spy-network-facebook-to-use-facial-recognition-technology-to-track-individuals-across-photos-videos.html.

138 KNOW PRIVACY, http://www.knowprivacy.org (last visited Nov. 20, 2013).

139 *See* United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (using peer-to-peer software); United States v. Courtney, No. 4:07CR261 JLH, 2008 U.S. Dist. LEXIS 109344, at *5-6 (E.D. Ark. Sept. 22, 2008) (employing chat rooms, Internet searches, and social networking sites); United States v. Carter, 549 F. Supp. 2d 1257, 1259-60 (D. Nev. 2008) (posting to a "hard core child pornography message board" links to a dummy website to record the IP addresses of users); *see also* United States v. Stults, 575 F.3d 834, 838 (8th Cir. 2009) (pinpointing location using ISP address only); *see generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 169, 175 (2004) ("[W]e are increasingly seeing collusion, partly voluntary, partly coerced, between the private sector and the government."); Brandon T. Crowther, Comment, *(Un)Reasonable Expectation of Digital Privacy*, 2012 BYU L. REV. 343, 359-60. *But see* Martin Kaste, *Google Explains How It Handles Police Requests for Users' Data*, NPR (Jan. 28, 2013, 3:34 AM), http://www.npr.org/2013/01/28/170428992/google-posts-how-it-handles-requests-for-users-data (reporting that Google recently posted a policy of requiring a warrant before law enforcement can access certain categories of material, possibly intended to "make it easier for the company to resist pressure from a government agency looking for quiet cooperation," as legal requirements for accessing online content are unclear).

140 Page, *supra* note 136; *see also* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 45 (2011) ("[W]hole categories of data are stored that never were before. If I wanted to purchase a book in a time not so distant, I would enter a bookstore, browse in a practically anonymous fashion, and make my purchase with cash. The bookstore made no record of my identity other than the fleeting and casual memory of the store clerk. But today if I want to purchase a book I am likely to do so online, where not only the bookstore, but also my Internet service provider and payment provider will make personal records. Indeed, the bookstore might not only record what books I ultimately purchase, but every book I peruse. And these records are stored in a

correlations among bits of information stored in various forms—including photographs taken from closed-circuit surveillance cameras, algorithms of facial images, phone call records, financial transactions, crime statistics, or email records—the government will soon be able to predict behavior before it happens,[141] much like Tom Cruise in the futuristic blockbuster *Minority Report*.[142]

C. *FRT: State-of-the-Art Menace?*

FRT produces uniquely powerful data for making correlations across exabytes of digital information. Humans engage in facial recognition instinctively by observing and identifying a person as being one they have seen before.[143] In addition to facial features, humans use clothing, gait, hair, posture, and other information about a subject's physical appearance for identification.[144] In automated systems, a device collects information about individuals and stores it in a database according to a numeric code or algorithm that represents the face—a "faceprint."[145] This can be done in a number of ways. One is to measure the distance between various "nodal points" or peaks and valleys on the face, such as the eyes, the width of nose, or the depth of the eye sockets, cheekbones, jawline, and chin.[146] The faceprint can also be generated by mapping the unique placement of pores, lines, and spots on the texture of an individual's skin.[147] The computer then searches the biometric database for comparisons of the newly acquired facial data to

---

digital format that permits, once an architecture has been established, essentially costless searching and distribution.").

141 Page, *supra* note 136; *see generally The Science of Civil War: What Makes Heroic Strife*, ECONOMIST (April 21, 2012), http://www.economist.com/node/21553006 (describing the development of computer models to predict the outbreak and spread of civil conflict).

142 *See generally* Roger Ebert, Review, *Minority Report*, ROGEREBERT.COM (June 21, 2012), www.rogerebert.com/reviews/minority-report-2002. *Person of Interest* is a modern series that is similarly premised on the ability of computers to predict crimes from data captured through omnipresent surveillance systems. Mary McNamara, *TV Review: 'Person of Interest,'* L.A. TIMES (Sept. 22, 2011), articles.latimes.com/print/2011/sep/22/entertainment/la-et-person-interest-20110922.

143 *See* Joyce W. Luk, Note, *Identifying Terrorists: Privacy Rights in the United States and the United Kingdom*, 25 HASTINGS INT'L & COMP. L. REV. 223, 230 (2002).

144 Antitza Dantcheva et al., Bag of Soft Biometrics for Person Identification: New Trends and Challenges 6-7 (Jan. 8, 2010) (manuscript), *available at* http://www.eurecom.fr/en/publication/3247/download/mm-publi-3247_1.pdf.

145 Luk, *supra* note 143, at 230.

146 *See* Susan McCoy, Comment, *O'Big Brother Where Art Thou? The Constitutional Use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUTER & INFO. L. 471, 477 (2002).

147 *See id.*

stored data.[148] FRT is capable of matching a face from a database of over 1.6 million photos with 92-percent accuracy.[149]

FRT is useful for two main purposes. The first is verification or authentication—that is, the "one-to-one" matching of a faceprint with an individual record to authenticate the person's identity. The system does not check every record in the database for a match—only that which corresponds to the identity the individual is claiming as his own.[150] FRT can thus be used to efficiently control access to secure facilities because it allows users to scan, verify, and store a face within a second and requires no physical touch, password, or employee badge.[151] The second use of FRT is for identification of an otherwise unknown individual from an anonymous image. For this function, the FRT system is provided an image and attempts to identify a different image of the same individual in the database through a "one-to-many" matching process.[152] Thousands of gigabytes of data are searched to retrieve all images that include a particular human subject. Typically, the computer produces a group of facial images ranked by computer-evaluated similarity. If a score is above a predetermined threshold, a match is identified.[153] In this way, FRT can be used to identify a particular individual or to create a profile of a random subject which could be useful for marketing and law enforcement purposes.

The private sector is rapidly realizing the commercial potential of FRT. Retailers use FRT to identify shoplifters.[154] Casinos use it to detect card counters and prevent their entry to the blackjack tables.[155] Airports, banks, museums, and factories have installed "walk through identification systems" that can identify sixty people per minute[156] and will eventually

---

148 *See generally* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1393 (2004).

149 *"Minority Report" Facial Recognition System Being Installed Across USA by FBI; Everyone to Be Tracked*, INT'L BUS. TIMES (Sept. 17, 2012, 1:04 PM), http://au.ibtimes.com/articles/384897/20120917/minority-report-facial-recognition-system-being-installed.htm#.UFcJLq6Sm70.

150 Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, CTR. FOR CATASTROPHE PREPAREDNESS & RESPONSE, 11 (2009).

151 *See* Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 325-26 (1999).

152 Introna & Nissenbaum, *supra* note 150, at 12.

153 *See id.*

154 Laura J. Nelson, *Instant Facial Recognition Tech a Two-Edged Sword*, L.A. TIMES (Nov. 14, 2012), http://articles.latimes.com/2012/nov/14/business/la-fi-face-first-20121114.

155 *See, e.g.*, *Visual Casino Suite 6*, BIOMETRICA, http://www.biometrica.com/products.html (last visited Nov. 20, 2013) (corporate website touting FRT product "Virtual Casino 6" for this purpose); Ellen Nakashima, *From Casinos to Counterterrorism*, WASH. POST (Oct. 22, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/10/21/AR2007102101522.html.

156 Press Release, Artec Grp., Artec ID Unveils Next Generation of Biometric 3D Facial Recognition Technology for High-Traffic Walk Through Identification Systems at ASIS International (Sept. 10,

operate at long distances.[157] Technology is being developed to automatically adapt videos into "avatar-sized images of just a user's face"[158] and to gauge the attractiveness of crowds.[159] In the near future, FRT will be embedded into signs and billboards to instantly scan faces, identify recent purchase history, and adjust the retailer's message to a person's tastes.[160] Restaurants and stores are already exploring uses of FRT to assimilate data from social media sites such as Facebook for this purpose.[161] Using only Facebook and commercially available FRT, researchers in 2012 were able to identify college students more than 30 percent of the time,[162] retrieving their names, photos, and other personal information from Facebook—including the first five digits of social security numbers—with the privacy settings turned on.[163]

Law enforcement now uses FRT systems "to identify suspects, accomplices and even innocent bystanders in a wide range of criminal investigations," with scant public notice.[164] The technology is highly efficient, allowing investigators to perform in a manner of minutes a review of surveillance video which might take hundreds of hours to manually com-

---

2012), *available at* http://www.marketwire.com/press-release/artec-id-unveils-next-generation-biometric-3d-facial-recognition-technology-high-traffic-1699489.htm.

157 Jim Spencer, *Facial Recognition: They Know Who You Are*, STAR TRIBUNE (last updated Aug. 17, 2012, 5:20 PM), http://www.startribune.com/business/166593666.html?refer=y (quoting a marketing director).

158 Sarah Perez, *Following Facebook's Shut Down of Face.com's Facial Recognition API, Lambda Labs Debuts an Open Source Alternative*, TECHCRUNCH.COM (Sept. 4, 2012), http://techcrunch.com/2012/09/04/following-facebooks-shut-down-of-face-coms-facial-recognition-api-lambda-labs-debuts-an-open-source-alternative/.

159 *See SceneTap: The Creepy App that Scans Bar-Goers' Faces*, THE WEEK (May 23, 2012), http://theweek.com/article/index/228281/scenetap-the-creepy-app-that-scans-bar-goers-faces.

160 Sarah Freishtat, *Just a Face in a Crowd? Scans Pick up ID, Personal Data*, WASH. TIMES (July 26, 2012), http://www.washingtontimes.com/news/2012/jul/26/just-a-face-in-a-crowd-scans-pick-up-id-personal-d/?page=all.

161 *See* Somini Sengupta & Kevin J. O'Brien, *Facebook Can ID Faces, but Using Them Grows Tricky*, N.Y. TIMES (Sept. 21, 2012), http://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html?_r=0 (noting that the developer Redpepper has stated that "users would have to authorize the application to pull their most recent tagged photographs"); Whitehead, *supra* note 3 ("[A] new Facebook application, Facedeals, is being tested . . . which enables businesses to target potential customers with specialized offers.").

162 Alessandro Acquisti, Ralph Gross & Fred Stutzman, Presentation, Faces of Facebook: Privacy in the Age of Augmented Reality (Aug. 4, 2011), *available at* http://www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf.

163 Bob Sullivan, *Researchers Say They Can Guess Your SSN*, NBCNEWS.COM (July 6, 2009, 7:59 PM), http://www.nbcnews.com/technology/researchers-say-they-can-guess-your-ssn-6C10406565.

164 Craig Timberg & Ellen Nakashima, *State Photo-ID Databases Become Troves for Police*, WASH. POST (June 16, 2013), http://articles.washingtonpost.com/2013-06-16/business/40012903_1_databases-facial-recognition-systems-searches.

plete.[165] Thirty-seven states now apply FRT to searchable databases containing the images of more than 120 million people from driver's license registries and non-driver identification cards.[166] Ten states have authorized FBI access to their data for investigative purposes.[167] All combined, federal and state FRT databases currently contain approximately 400 million facial images.[168] The most advanced systems enable officers to run searches of this data from laptops in squad cars.[169]

In addition to photos obtained from passports, drivers' licenses, and mug shots, the government is collecting countless video and still images of the general public from surveillance cameras in public locations and other sources. A company named Trapwire is working with police from the District of Columbia, New York, and Los Angeles on rapid analysis of live footage from closed-circuit TV surveillance cameras,[170] which number in the thousands in the New York City subway system alone.[171] Undercover police in Florida have reportedly "mingl[ed] with the public, using their smartphones to take videos and photos," and then checked images against FRT data to pull up names and identities.[172] At the 2012 Republican National Convention in Tampa, live videos from smartphones fed into a surveillance system that included ninety-four high-definition cameras.[173] The Federal Communications Commission gave permission to test this surveillance system as "part of an effort to eventually develop a similar $7 billion National Public Safety Broadband Network [of] highly secure, encrypted voice, video, and data communications, as well as an evidence-quality,

---

165 Mariel Myers, *Boston Bombings: How Facial Recognition Can Cut Investigation Time to Seconds*, CNET.COM (April 18, 2013, 5:56 PM), http://news.cnet.com/8301-1009_3-57580367-83/boston-bombings-how-facial-recognition-can-cut-investigation-time-to-seconds/.

166 Timberg & Nakashima, *supra* note 164.

167 *Id.*

168 *Id.*

169 *Id.* The software of a single private contractor, MorphoTrust USA, operates in most government FRT systems. *Id.*

170 Whitehead, *supra* note 3.

171 Jesus Diaz, *FBI's Sinister New $1 Billion Project Will Track Everyone by Their Face*, GIZMODO (Sept. 10, 2012, 1:44 PM), http://gizmodo.com/5941926/fbis-sinister-new-1-billion-project-will-track-everyone-by-their-face. In August 2012, the New York Police Department ("NYPD") partnered with Microsoft to launch what it calls a "Domain Awareness System," which analyzes data collected from 3,000 closed-circuit video cameras, records of 911 calls, license plate readers, historical crime reports, and radiation sensors throughout the city. The NYPD can now instantly track where a particular vehicle has been in recent days or weeks, pull up the driver's arrest records and related 911 calls, and map his criminal history "to geospacially and chronologically reveal crime patterns." Page, *supra* note 136.

172 Darlene Storm, *Undercover Cops Secretly Use Smartphones, Face Recognition to Spy on Crowds*, COMPUTERWORLD (Sept. 18, 2012, 12:50 PM), http://blogs.computerworld.com/privacy/21010/undercover-cops-secretly-use-smartphones-face-recognition-spy-crowds.

173 *Id.* Older video cameras did not have the resolution or connectivity to work with FRT. Diaz, *supra* note 171.

permanent recording of all data collected."[174] The government's access to real-time data will soar as upwards of thirty thousand surveillance drones are launched in the next decade,[175] many by private sector corporations. Equipped with powerful FRT cameras, the drones "will be capable of capturing minute details, including every mundane action performed by every person in an entire city simultaneously."[176]

At the federal level, the FBI has undertaken a billion-dollar effort to expand its current fingerprint database into a Next Generation Identification ("NGI") system that will include data such as iris scans, photos, palm prints, gait and voice recordings, scars, tattoos, and DNA.[177] "NGI will use a variety of biometric data, cross-referenced against the nation's growing network of surveillance cameras to not only track your every move but create a permanent 'recognition' file on you within the government's massive databases."[178] The plan is for NGI to be "fully operational in 2014," and to share its information with other federal agencies and the states.[179]

Additionally, government FRT systems have access to private sector sources of images—including private cell phones and social networking websites—for use in identifying subjects.[180] Facebook's "tag suggestion" function automatically retrieves the names of individuals in photos uploaded by its one billion users at a rate of three hundred million a day.[181] Although Facebook made a statement to Congress that it "store[s FRT] templates in encrypted form and maintain[s] them in a monitored and access-

---

174 Storm, *supra* note 172 (quoting Josh Smith, *Undercover Police Used Smartphones to Keep Tabs on Protests in Tampa*, NAT'L J. (Sept. 17, 2012), http://www.nationaljournal.com/tech/smartphones-used-to-monitor-tampa-protests-20120917) (internal quotation marks omitted).

175 Whitehead, *supra* note 3.

176 *Id.*

177 *Id.*; *see* David Jeffers, *FBI Rolling Out High-Tech 'Big Brother' Monitoring System*, PC WORLD (Sept. 10, 2012, 6:58 AM), http://www.pcworld.com/article/262071/fbi_rolling_out_hightech_big_brother_monitoring_system.html. In 2002, it was reported that the Department of Defense was similarly developing a Total Information Awareness project that would consist of a huge database of personal financial, educational, health, and travel information about individuals, obtained from private sector companies. In response to a public outcry, Congress voted to deny funding for the initiative. Shannon R. Anderson, *Total Information Awareness and Beyond: The Dangers of Data Mining Technology to Prevent Terrorism*, BILL OF RTS. DEF. COMM., 3 (July 26, 2004), http://www.bordc.org/data-mining.pdf.

178 Whitehead, *supra* note 3.

179 *Id.*

180 The FBI claims not to be mining such data at this time. *See* Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. TIMES (Sept. 9, 2007), http://www.nytimes.com/2007/09/09/washington/09fbi.html?pagewanted=all. With an FRT search from his smartphone, a detective in Carlisle, Pa., recently identified a suspect by linking a Facebook image with a mug shot database. Timberg & Nakashima, *supra* note 166.

181 Sengupta & O'Brien, *supra* note 161.

restricted database,"[182] its current privacy policy reserves a right to "access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address . . . illegal activity" or "to protect ourselves, you and others."[183] It was recently disclosed that the National Security Agency's ("NSA") Prism program enables direct government access to the systems of Google, Apple, Facebook, and other Internet companies for purposes of obtaining search histories, email content, file transfers, and live chats.[184] Government agencies also collaborate with private entities through a network of federally funded "fusion centers" for mining collective databases and histories of online activity.[185]

The law enforcement and national security benefits of using FRT in targeted criminal investigations are self-evident.[186] But its potential for enabling surveillance of common citizens is troubling. Before FRT, drivers' license photos were of limited utility to investigators unless a subject's name was already known.[187] Law enforcement can now capture a facial image of an *unknown* individual without the subject's knowledge, match the image with other bits of data using FRT algorithms, and come up with a rich dossier of personal information.[188] Although fingerprint data similarly enables investigators to attach a name to unidentified biometric data,[189] FRT

---

182 *Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties," Before the Subcomm. on Privacy, Tech. and the Law of the S. Judiciary Comm.*, 112th Cong. 1 (2012) (questions for the record from Sen. Al Franken for Rob Sherman), *available at* http://www.judiciary.senate.gov/resources/transcripts/upload/071812QFRs-Sherman.pdf.

183 *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/other (last visited Nov. 20, 2013).

184 Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013), http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data. Section 702 of the FISA Amendments Act, 50 U.S.C. § 1881a, authorizes intelligence-gathering on non-U.S. citizens for up to a year and has been cited by Director of National Intelligence James Clapper as the legal authority for the Prism program. Sam Stein, *PRISM Program: Obama Administration Held 22 Briefings for Congress on Key FISA Law*, HUFFINGTON POST (June 10, 2013, 4:01 PM), http://www.huffingtonpost.com/2013/06/10/prism-program-obama_n_3416973.html.

185 Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 264 (2013).

186 *See* Press Release, Iowa State Univ., Iowa State Professor Weighs Benefit vs. Risk of Facial Recognition Technology (May 8, 2013), *available at* http://www.news.iastate.edu/news/2013/05/08/facialrecognition.

187 *See* Timberg & Nakashima, *supra* note 166 ("The increasingly widespread deployment of the technology in the United States has helped police find murderers, bank robbers and drug dealers, many of whom leave behind images on surveillance videos or social-media sites that can be compared against official photo databases.").

188 *Id.* At this point, "[a]n affidavit for a warrant could then be automatically generated, electronically signed and forwarded to a judge. Once granted, investigators could use a code to enter an encrypted portal to the telephone service provider and get GPS coordinates that lead right to the suspect." Page, *supra* note 136.

189 *See* Maryland v. King, 133 S. Ct. 1958, 1987 (2013) (Scalia, J., dissenting) ("Fingerprints of arrestees are taken primarily to identify them (though that process sometimes solves crimes) . . . .").

goes much further. Once a person is identified, rapid correlations with countless other images and data points in cyberspace and self-contained databases can detect past activity and predict future movements.[190] Taken to its extreme, this technology could be used to perform "identity sweeps" of random subjects for relatively benign activities like walking a dog without a leash.[191] A few states have imposed legislative barriers to police collection of and access to FRT data, but many others have not.[192] The feasibility of domestic "police state" surveillance operations is thus no longer a matter of science fiction.[193] FRT renders innocent people susceptible to intrusive police investigations for being "tagged" in a photo with someone suspected of a crime.[194]

Although the FBI currently limits the use of FRT to finding potential leads,[195] there remains significant potential for errors and abuse.[196] Match errors occur in the form of false positives and false negatives. A false positive occurs where the FRT system incorrectly declares a successful match when the images are not of the same individual.[197] A false negative occurs where the FRT system fails to declare a match when the images are, in fact, of the same individual.[198] Image quality, the background environment, the movement and age of the subject, the focus and quality of the camera, lighting, and the angle at which the subject's image is captured all contribute to match errors.[199] If a face or set of features is altered with a disguise or hat, the likelihood of misidentification increases.[200] Yet law enforcement officers rely on electronic matches of photographs and images in the FBI's existing database without any human verification of the results.[201] And as a re-

---

190 *See generally id.* (discussing the distinction between fingerprinting and DNA analysis for purposes of solving crimes versus verifying identities).

191 Timberg & Nakashima, *supra* note 166.

192 *Id.*

193 *Id.*

194 *Id.* In the European Union, Facebook turned off its FRT after regulators deemed it a threat to privacy. Chris Smith, *Facebook Turns Off Facial Recognition Tech in EU*, TECHRADAR.COM (Sept. 22, 2012), http://www.techradar.com/us/news/internet/web/facebook-turns-off-facial-recognition-tech-in-eu-1099104; *see also* Sengupta & O'Brien, *supra* note 161 (noting that Facebook also agreed to "delete the data used to identify Facebook users by their pictures"); Blue, *supra* note 47 (discussing actions by other EU countries). A Washington, D.C., advocacy group has filed a complaint against Facebook with the Federal Trade Commission over its tagging feature. Sengupta & O'Brien, *supra* note 161.

195 Spencer, *supra* note 157.

196 Whitehead, *supra* note 3.

197 JOHN VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 376 (2007).

198 *Id.*

199 Introna & Nissenbaum, *supra* note 150, at 3, 18, 38-39.

200 Richa Singh, Mayank Vatsa & Afzel Noore, Recognizing Face Images with Disguise Variations 149, 151, 156 (June 1, 2008) (manuscript), *available at* http://cdn.intechopen.com/pdfs/5898/InTech-Recognizing_face_images_with_disguise_variations.pdf.

201 Madison Ruppert, *FBI Sharing Facial Recognition Software with Police Departments Across America*, END THE LIE (Aug. 24, 2012), http://endthelie.com/2012/08/24/fbi-sharing-facial-recognition-

sult of what is known as "function creep" or "mission creep," the initial purpose for lawfully collecting images may later morph into additional uses that were unannounced or unintended.[202] These vulnerabilities have serious implications, even for those with no reason to fear law enforcement.

D. *The Harms of Compromised Anonymity*

In the big data universe, FRT enables users to trace a passerby's life in real time—past, present, and future—through the relation of faceprint algorithms with other data points. Although the American public's reaction to the NSA's Prism program was relatively muted,[203] most people understand the awkward feeling of being stared at on a bus.[204] Constant surveillance by the government is more pernicious. It discovers a person's identity and then augments that information based on intelligence that today's technology renders limitless. The loss of anonymity that results from the detailed construction of a person's identity through ongoing monitoring can lead to at least three categories of harm, discussed below.

First, as the panopticon suggests, ongoing identification and tracking can adversely influence behavior. People involuntarily experience "self-

---

software-with-police-departments-across-america/#axzz2fwTGPWgr. The FBI has indicated that only authorized law enforcement agencies have access to its data, which does not currently include photos from social media sites. Critics claim, however, that the FBI does intend to search social media sites with FRT technology. Kathleen Hickey, *FBI to Open Facial Recognition Searches to Police Nationwide*, GCN.COM (Aug. 20, 2012), http://gcn.com/articles/2012/08/20/fbi-facial-recognition-software-open-to-police.aspx.

202 The sole purpose of the creation of social security numbers, for example, was to facilitate record keeping and determine the amount of social security taxes to credit to each contributor's account. By 1961, however, the IRS began using social security numbers for tax identification purposes. *See* Bijon Roy, *A Case Against Biometric National Identification Systems (NIDS): "Trading-Off" Privacy Without Getting Security*, 19 WINDSOR REV. LEGAL & SOC. ISSUES 45, 75-76 (2005); *see also* Tom Cheshire, *25 Big Ideas for 2012: Ubiquitous Face Recognition*, WIRED (Jan. 9, 2012, 9:22 AM), http://www.wired.com/business/2012/01/ubiquitous-face-recognition (noting that there are concerns over FRT mission creep and quoting a security technology expert as saying that "[r]ecognizing people in photographs works well . . . [b]ut attempts to pick terrorists out of crowds have failed, resulting in systems that do a great job surveilling innocents and a terrible job identifying the guilty" (internal quotation marks omitted)).

203 PEW RESEARCH CENTER, PUBLIC SAYS INVESTIGATE TERRORISM, EVEN IF IT INTRUDES ON PRIVACY: MAJORITY VIEWS NSA PHONE TRACKING AS ACCEPTABLE ANTI-TERROR TACTIC 1 (2013), *available at* http://www.people-press.org/files/legacy-pdf/06-10-13%20PRC%20WP%20Surveillance%20Release.pdf (reporting that, as of June 2013, 56 percent of Americans believe that Prism is an acceptable way for the government to investigate terrorism).

204 Many cities have begun equipping buses with security cameras. William Neuman, *Equipment Problems Delay Plan for Cameras on Buses*, N.Y. TIMES (March 29, 2007), http://www.nytimes.com/2007/03/29/nyregion/29bus.html?_r=0.

censorship and inhibition" in response to the feeling of being watched.[205] They "might think twice," for example, "before visiting websites of extreme sports or watching sitcoms glorifying couch potatoes if they felt this might result in higher insurance premiums."[206] The social norms that develop around expectations of surveillance can, in turn, become a tool for controlling others. To be sure, social control is beneficial for the deterrence of crime and management of other negative behavior. Too much social control, however, "can adversely impact freedom, creativity, and self-development."[207] Professor Jeffrey Rosen has explained that the pressures of having one's private scandals "outed" can push people toward socially influenced courses of action that, without public disclosure and discussion, would never happen.[208] They are less willing to voice controversial ideas or associate with fringe groups for fear of bias or reprisal.[209] With the sharing of images online, the public contributes to what commentators have called "sousveillance" or a "reverse Panopticon" effect, whereby "the watched become the watchers."[210]

Second, dragnet-style monitoring can cause emotional harm. Living with constant monitoring is stressful, inhibiting the subject's ability to relax and negatively affecting social relationships.[211] When disclosures involve particularly sensitive physical or emotional characteristics that are normally concealed—such as "[g]rief, suffering, trauma, injury, nudity, sex, urination, and defecation"—a person's dignity and self-esteem is affected, and incivility toward that person increases.[212]

Third, constant surveillance through modern technologies reduces accountability for those who use the data to make decisions that affect the people they are monitoring.[213] The collection of images for FRT applica-

---

205 ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 17 (2011) (quoting Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1418 (2001)) (internal quotation marks omitted). In 1897, a study found that the presence of other riders caused cyclists to pedal faster. Matthew Lynch, *Closing the Orwellian Loophole: The Present Constitutionality of Big Brother and the Potential for a First Amendment Cure*, 5 FIRST AMENDMENT L. REV. 234, 271 & n.136 (2007) (citing Norman Triplett, *The Dynamogenic Factors in Pacemaking and Competition*, 9 AM. J. PSYCHOL. 507, 533 (1898)); *see also* Slobogin, *supra* note 23, at 242-47, 251 (describing empirical research on the effects of being watched).

206 MAYER-SCHÖNBERGER & CUKIER, *supra* note 11, at 57.

207 Solove, *supra* note 17, at 494.

208 Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 GEO. L.J. 2117, 2122 (2001).

209 *See* Slobogin, *supra* note 23, at 217; *infra* Part II.B (discussing FRT and the First Amendment).

210 Carla Scherr, Note, *You Better Watch Out, You Better Not Frown, New Video Surveillance Techniques Are Already in Town (and Other Public Spaces)*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 499, 505 (2007) (internal quotation marks omitted).

211 Solove, *supra* note 17, at 555.

212 *Id.* at 536-37.

213 *Id.* at 508-09, 523; *cf. id.* at 509 (discussing *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), in which the Supreme Court found that

tions is indiscriminate, with no basis for suspecting a particular subject of wrongdoing. It allows users to cluster disparate bits of information together from one or more random, unidentified images such that "[t]he whole becomes greater than the parts."[214] The individuals whose images are captured do not know how their data is being used and have no ability to control the manipulation of their faceprints, even though the connections that are made reveal new facts that the subjects did not knowingly disclose. The party doing the aggregating gains a powerful tool for forming and disseminating personal judgments that render the subject vulnerable to public humiliation and other tangible harms, including criminal investigation.[215] Incorrect surveillance information can lead to lost job opportunities, intense scrutiny at airports, false arrest, and denials of public benefits.[216] In turn, a lack of transparency, accountability, and public participation in and around surveillance activities fosters distrust in government. The recent scandal and fractured diplomatic relations over NSA surveillance of U.S. allies is a case in point.[217] Perhaps most troubling, FRT enhances users' capacity to identify and track individuals' *propensity* to take particular actions,[218] which stands in tension with the common law presumption of innocence embodied in the Due Process Clause of the Fifth and Fourteenth Amendments.[219] As described below, prevailing constitutional doctrine does not account for the use of technology to identify, track, and predict the behavior of a subject using an anonymous public image and big data correlations.

II. ANONYMITY AND THE CONSTITUTION

Although the Constitution lacks an express right to privacy, the Supreme Court has acknowledged that the Bill of Rights reflects the Framers' concern for protecting specific aspects of physical privacy, such as privacy

---

disclosure of FBI rap sheets containing aggregated information—otherwise public—violated a privacy exemption of the Freedom of Information Act).

214 *Id.* at 507.

215 *Id.* at 508-09, 523.

216 *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1274 (2008).

217 *See* Ken Dilanian & Janet Stobart, *White House OKd Spying on Allies, U.S. Intelligence Officials Say*, L.A. TIMES (Oct. 28, 2013, 7:25 PM), http://www.latimes.com/world/la-fg-spying-phones-20131029,0,3235295.story#axzz2jEB9FaoQ.

218 *See The 'Big Data' Revolution: How Number Crunchers Can Predict Our Lives*, NPR.ORG (Mar. 7, 2013, 3:00 AM), http://www.npr.org/2013/03/07/173176488/the-big-data-revolution-how-number-crunchers-can-predict-our-lives (reporting that law enforcement is already engaged in predictive policing).

219 *See* Estelle v. Williams, 425 U.S. 501, 503 (1976) ("The right to a fair trial is a fundamental liberty secured by the Fourteenth Amendment. The presumption of innocence, although not articulated in the Constitution, is a basic component of a fair trial under our system of criminal justice." (citation omitted)).

of speech and assembly (First Amendment),[220] privacy of the home against demands that it be used to house soldiers (Third Amendment),[221] privacy of the person and possessions against unreasonable searches (Fourth Amendment),[222] and informational privacy (Fifth Amendment privilege against self-incrimination).[223] Many view the splintered decision in *Griswold v. Connecticut*[224] as the Supreme Court's first recognition of a right to decisional privacy[225] on the theory that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance," and that some of those guarantees "create zones of privacy."[226] Writing for a majority of which two Justices concurred only in the judgment, Justice Douglas construed such penumbras to include the First Amendment's right of association and the Fourth Amendment's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[227] Although the Supreme Court has steadily reviewed new surveillance technologies under the Fourth Amendment for more than a century, prevailing doctrine leaves FRT beyond constitutional scrutiny. By contrast, anonymity is an interest that has received First Amendment protection, but no court has extended that doctrine to

---

220 U.S. CONST. amend. I.

221 U.S. CONST. amend. III.

222 U.S. CONST. amend. IV.

223 U.S. CONST. amend. V. Although the Fifth Amendment protects against compelled testimonial incrimination, it does not apply to compulsory fingerprinting, photographing, taking measurements, writing or speaking for identification purposes, having bodily fluids drawn, or DNA evidence because they are not evidence of a communicative or testimonial nature. *See* Schmerber v. California, 384 U.S. 757, 760-61, 764 (1966); Shaffer v. Saffle, 148 F.3d 1180, 1181 (10th Cir. 1998). FRT is capable of more than simply identifying a person's face. It can be used to identify an individual as being at a specific location at a specific time. The Fifth Amendment, however, does not limit the government's collection of FRT data from private sources, or its subsequent use of FRT for identification and surveillance of individuals. The Supreme Court has repeatedly stated that "a party incriminated by evidence produced by a third party sustains no violation of his own Fifth Amendment rights." Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 55 (1974) (citing additional cases). Hence, the Fifth Amendment does not protect against subpoenas for a person's records and papers held by third parties. Couch v. United States, 409 U.S. 322, 328, 333-35 (1973).

224 381 U.S. 479 (1965).

225 *See generally* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1089 (2006) (book review) ("Decisional privacy is usually defined as the right of individuals to make certain kinds of fundamental choices with respect to their personal and reproductive autonomy . . . .").

226 *Griswold*, 381 U.S. at 484; *see also* Whalen v. Roe, 429 U.S. 589, 599 n.25 (1977) (quoting *Griswold* in Fourth Amendment case); *Cal. Bankers*, 416 U.S. at 78-79 (Powell, J., concurring) ("Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy."). In subsequent decisions, the privacy right has come to encompass matters such as child rearing, procreation, and termination of medical treatment as a matter of due process. Bowers v. Hardwick, 478 U.S. 186, 190 (1986), *overruled by* Lawrence v. Texas, 539 U.S. 558 (2003).

227 *Griswold*, 381 U.S. at 484 (quoting U.S. CONST. amend. IV) (internal quotation marks omitted).

government surveillance methods.[228] Thus, as things stand, the Constitution plays no meaningful role in confining the serious anonymity harms associated with FRT identification and monitoring.

A. *Anonymity and the Fourth Amendment*

The Supreme Court has recognized that "[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[229] In *Mapp v. Ohio*,[230] the Court characterized the Fourth Amendment as actually establishing a "right to privacy, no less important than any other right carefully and particularly reserved to the people."[231] Together with the Fifth Amendment,[232] the Fourth Amendment "express[es] 'supplementing phases of the same constitutional purpose—to maintain inviolate large areas of personal privacy.'"[233] Application of traditional Fourth Amendment doctrine to modern surveillance technologies such as FRT nonetheless risks emptying such privacy guarantees of meaning.

Numerous scholars have addressed whether the Fourth Amendment covers the government's use of novel technologies, and how leading doctrine should be adjusted to ensure sufficient constitutional scrutiny of new methods of conducting a law enforcement "search."[234] This Section highlights an additional nuance that warrants consideration within this discussion: a distinction between pre-digital and digital age cases. The surveillance potential of big data was only technologically possible after the Internet took hold on the public with the development of the first webpage and web browsers in the early 1990s.[235] Today, it is technology's capacity to generate new information by making correlations among individual data points which poses unprecedented threats to the ability to remain anonymous in modern society, rendering traditional Fourth Amendment doctrine

---

228 Blitz, *supra* note 148, at 1381.

229 Schmerber v. California, 384 U.S. 757, 767 (1966).

230 367 U.S. 643 (1961).

231 *Id.* at 656.

232 *See supra* note 223.

233 *Mapp*, 367 U.S. at 657 (quoting Feldman v. United States, 322 U.S. 487, 489-90 (1944), *overruled in part by* Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 74-75 (1964)).

234 *See, e.g.*, Gutterman, *supra* note 103, at 651 (arguing that "fourth amendment jurisprudence will be best served by adhering to a 'value-dominated model' that is capable of reconciling the competing privacy interests with modern technological surveillance"); Kerr, *supra* note 125, at 311 (analyzing a "'mosaic theory' of the Fourth Amendment, by which courts evaluate a collective sequence of government activity as an aggregated whole to consider whether the sequence amounts to a search").

235 *See* Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 WIDENER L.J. 667, 669 (2006) (characterizing twenty-first century "pervasive technology" as the "antithesis of context-specific technologies such as rail transportation" and observing that "the goal and practice of pervasive technology is to integrate sophisticated interactive technologies into the fabric of our daily lives").

outmoded for the digital age. As explained below, a contingent of the Supreme Court is beginning to recognize that constitutional doctrine must be adapted to establish boundaries on the use of technology for constant surveillance of the general public.

1. Pre-Digital Age

The categorization of government activity as a search under the Fourth Amendment is important under traditional doctrine: if something is not a search, the analysis ends, and the government is not required to show probable cause.[236] A traditional search is like the tort of trespass, which existed at the time the Fourth Amendment was adopted. It involves a physical intrusion on private property. The Supreme Court deviated from this property-based approach to determining whether something is a search early on, however, and developed a "reasonable expectation of privacy" trigger.[237] In the absence of a trespass, "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[238] The legitimate expectation of privacy in a searched person or location must meet both a subjective and an objective test of reasonableness. "[F]irst, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?"[239] For subpoenas, the Court has invoked the Fourth Amendment only minimally, applying a reasonableness test that is satisfied if a subpoena is not "too sweeping in its terms."[240] It has also authorized warrantless searches in three circumstances: if there is "reasonable suspicion" of a past or imminent crime to justify a stop and frisk;[241] if "'special needs' other than the normal need for law enforcement provide sufficient justification" for a search,[242] as in cases of mandatory drug testing for employment or in schools;[243] and if a regulatory scheme

---

236 *See, e.g.*, Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (concluding the Fourth Amendment analysis when aerial surveillance was found not to be a search).

237 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

238 Kyllo v. United States, 533 U.S. 27, 31-33 (2001).

239 California v. Ciraolo, 476 U.S. 207, 211 (1986).

240 Hale v. Henkel, 201 U.S. 43, 76 (1906), *overruled in part on other grounds by* Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 69 (1964); *see also* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 4.13(a) (5th ed. 2012) ("Although the Supreme Court has stated in dicta that the Fourth Amendment continues to limit the subpoena power of the government, the Court has rejected Fourth Amendment objections to subpoenas in every case it has decided in modern times." (footnote omitted)).

241 Terry v. Ohio, 392 U.S. 1, 27 (1968). Reasonable suspicion is a lower standard than probable cause; it requires "specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion." *Id.* at 22.

242 Ferguson v. City of Charleston, 532 U.S. 67, 74 n.7 (2001).

243 Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 633-34 (1989) (employment); New Jersey v. T.L.O., 469 U.S. 325 (1985) (schools).

authorizes warrantless inspections of property "for compliance with health and safety standards,"[244] for example. Additionally, the Court has established a status-based continuum of diminished privacy rights under the Fourth Amendment which includes "parolees hav[ing] fewer expectations of privacy than probationers."[245]

The question of what "privacy" means under the Fourth Amendment has nonetheless been in flux from the phrase's inception.[246] In *Olmstead v. United States,*[247] Louis Brandeis famously dissented from the majority's holding that wiretapping was not a Fourth Amendment violation absent physical trespass to the home, employing his familiar theory that "[t]he makers of our Constitution . . . conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[248] Employing a property-based approach to the Fourth Amendment, *Boyd v. United States*[249] marked a high point of the Supreme Court's recognition of broad protections against government invasion of privacy under the Fourth Amendment. In refusing to uphold a court order directing a defendant in a civil forfeiture proceeding to produce documentary evidence of liability, the Court framed the "essence" of the government's offense as "the invasion of [the] indefeasible right of personal security, personal liberty and private property," as the framers were keenly attuned to "[t]he struggles against arbitrary power in which they had been engaged for more than 20 years" when they approved the Fourth and Fifth Amendments.[250]

In *Katz v. United States*,[251] however, a majority of the Court rejected the property-based reasoning of *Boyd* and held that the relevant Fourth Amendment inquiry is whether the practice at issue "violated the privacy upon which [the defendant] justifiably relied."[252] It wrote that the Constitu-

---

244 Whren v. United States, 517 U.S. 806, 811 n.2 (1996).

245 Samson v. California, 547 U.S. 843, 850 (2006); *see generally* Rachael A. Lynch, Note, *Two Wrongs Don't Make a Fourth Amendment Right:* Samson *Court Errs in Choosing Proper Analytical Framework, Errs in Result, Parolees Lose Fourth Amendment Protection*, 41 AKRON L. REV. 651, 669-70 (2008) (noting that "parolees have an expectation of privacy somewhere between that of a probationer and a prisoner" (footnote omitted)).

246 An originalist might interpret the Constitution to argue that no general right to privacy exists beyond the specific Bill of Rights guarantees because, among other reasons, no such right is expressed in the plain language of the Constitution. *See* Peter J. Smith, *How Different Are Originalism and Non-Originalism?*, 62 HASTINGS L.J. 707, 711 (2011).

247 277 U.S. 438 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

248 *Id.* at 478 (Brandeis, J., dissenting).

249 116 U.S. 616 (1886).

250 *Id.* at 630; *see generally* Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 998 (1982) (construing *Boyd* as treating property as coextensive with personal privacy under the Fourth Amendment).

251 389 U.S. 347 (1967).

252 *Id.* at 353.

tion "protects people, not places."[253] Thus, the government violated the Fourth Amendment in electronically listening to and recording the defendant's conversation in a public telephone booth—once a fixture on American street corners and in Superman comics. The Court found it insignificant that the electronic device did not penetrate the structure's walls.[254] In doing so, the Court rejected the property-based approach to electronic surveillance, instead embracing Brandeis's articulation of the "right to be let alone."[255] It has restated this refrain many times since.[256]

Despite the doctrinal shift in *Katz,* existing Fourth Amendment doctrine provides no clear protection from government surveillance conducted through an amalgamation of FRT algorithms and other data. That Court made clear that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[257] Accordingly, the Court has held that, because "[t]he exterior of a car . . . is thrust into the public eye, . . . to examine it does not constitute a 'search.'"[258] Nor is there a reasonable expectation of privacy in the phone numbers "voluntarily conveyed . . . to the telephone company and 'exposed' . . . in the ordinary course of business."[259] There is no reasonable expectation of privacy in abandoned property, like garbage left out for collection,[260] or in the movements of an automobile on public thoroughfares.[261]

As a consequence, the collection of a faceprint does not constitute a search under the Court's longstanding view that "mere visual observation does not constitute a search."[262] Non-consensual facial scanning amounts to

---

253 *Id.* at 351.

254 *Id.* at 353.

255 *Id.* at 350.

256 *See, e.g.*, Doe v. Bolton, 410 U.S. 179, 213 (1973) (Douglas, J., concurring) ("[The] right of privacy . . . includes the privilege of an individual to plan his own affairs, for, ' "outside areas of plainly harmful conduct, every American is left to shape his own life as he thinks best, do what he pleases, go where he pleases." " (citation omitted) (quoting Kent v. Dulles, 357 U.S. 116, 126 (1958))); Eisenstadt v. Baird, 405 U.S. 438, 453 n.10 (1972) (quoting Stanley v. Georgia, 394 U.S. 557, 564 (1969)); *Stanley*, 394 U.S. at 564 ("[A]lso fundamental is the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy."); Time, Inc. v. Hill, 385 U.S. 374, 413 (1967) (Fortas, J., dissenting) ("[The right to privacy] is, simply stated, the right to be let alone; to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law.").

257 *Katz*, 389 U.S. at 351.

258 New York v. Class, 475 U.S. 106, 114 (1986).

259 Smith v. Maryland, 442 U.S. 735, 744 (1979).

260 California v. Greenwood, 486 U.S. 35, 43 (1988).

261 United States v. Knotts, 460 U.S. 276, 281 (1983).

262 United States v. Jones, 132 S. Ct. 945, 953 (2012); *see generally* Douglas A. Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places*, 16 VA. J.L. & TECH. 430, 441 (2011) (analyzing FRT under Fourth Amendment law and suggesting that "[g]overnment agencies have a strong argument . . . that where people lack an expectation of not being *observed*, they equally lack an expectation of not being *recognized*"); Scherr, *supra* note 210, at 508

no more than visual observation of what is held out to the public. To the extent that FRT is considered part and parcel of the traditional visual surveillance that police conduct in unmarked vehicles—which has long been considered constitutional[263]—the Fourth Amendment does not apply. FRT also targets an area of the body that a person would not reasonably expect to consider private. The Court has held that the taking of a photograph does not constitute a search because "[i]t does not involve a physical intrusion onto the person" and does not "invade[] any recognized 'expectation of privacy.'"[264] Insofar as FRT enables law enforcement to identify a subject from an anonymous photo, moreover, *Hiibel v. Sixth Judicial District Court*[265] suggests that such identification is constitutional.[266] There, the Court rejected a Fourth Amendment challenge to a law requiring people to identify themselves during a police stop on the theory that "[a]nswering a request to disclose a name is likely to be so insignificant in the scheme of things as to be incriminating only in unusual circumstances."[267] In dissent, Justice Stevens highlighted the ability to attach a name to "a broad array of information about the person" which, "in turn, can be tremendously useful in a criminal prosecution."[268]

Even if the Fourth Amendment were construed to broaden the meaning of "search" to encompass FRT, it would be an empty victory for privacy advocates. Many smartphones contain FRT technology,[269] and private citizens snap and upload countless images onto Facebook each day. Aside from the Thirteenth Amendment's ban on slavery,[270] the Constitution—and thus Brandeis's constitutional formulation of a right to be let alone—applies *only* "as against the Government."[271] If private parties employ FRT, the Constitution is not triggered. Those concerned that government will obtain

---

(arguing that video surveillance of actions within plain view is not covered by the Fourth Amendment); Alexander T. Nguyen, Comment, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, VA. J.L. & TECH., Spring 2002, at 1, 7 (arguing that the Fourth Amendment "seems useless" in the context of FRT).

263 *See* California v. Ciraolo, 476 U.S. 207, 213 (1986) (noting that officers can make observations from public vantage points).

264 Maryland v. King, 133 S. Ct. 1958, 1986 (2013) (Scalia, J., dissenting) (quoting Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)) (citing Florida v. Jardines, 133 S. Ct. 1409, 1413-14 (2013)).

265 542 U.S. 177 (2004).

266 *Id.* at 191.

267 *Id.*

268 *Id.* at 196 (Stevens, J., dissenting).

269 By 2017, it is expected that 665 million smartphones and tablets will have FRT. Spencer, *supra* note 157.

270 U.S. CONST. amend. XIII. There are also relatively rare exceptions under the state action doctrine. *See generally* Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1412 (2003) (describing state action doctrine).

271 Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347, 353 (1967).

existing FRT data through private channels have no apparent constitutional remedy if governmental use of such data effectively results in indiscriminate, twenty-four hour passive surveillance.

Relatedly, the Supreme Court "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[272] There is no Fourth Amendment ban on the use of information obtained through government informants, for example,[273] even though they "frustrat[e] actual expectations of privacy."[274] The Court has also upheld the warrantless installation of pen registers to record numbers dialed from a subject's home on the theory that "telephone subscribers [do not] harbor any general expectation that the numbers they dial will remain secret."[275] It has condoned government scrutiny of documents provided to accountants,[276] banks,[277] and physicians,[278] because such documents "contain only information voluntarily conveyed" and the individual "takes the risk . . . that the information will be conveyed by that person to the Government."[279] With the advent of the Internet, lower courts have applied the third-party doctrine to justify government subpoenas of shared computer files, information sent or received through the Internet and stored on a third-party server,[280] and individual subscriber information obtained from Internet service providers without a

---

272 United States v. Miller, 425 U.S. 435, 443 (1976) (citing United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).

273 *White*, 401 U.S. at 748-49; *see also Hoffa*, 385 U.S. at 302 (no Fourth Amendment protection for conversations with a colleague who turns out to be a government agent); Lewis v. United States, 385 U.S. 206, 210 (1966) (same regarding interactions with secret agent sent by the government to purchase narcotics from defendant); *Lopez*, 373 U.S. at 437 (same regarding agent's use of electronic recording equipment).

274 *White*, 401 U.S. at 752; *see generally* Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 566-70 (2009) (discussing cases and arguing in favor of third party doctrine as it "ensures technological neutrality of the Fourth Amendment by blocking the opportunistic use of third parties to circumvent the basic balance of Fourth Amendment rules" and because it "is needed to provide ex ante clarity"). *Compare* Henderson, *supra* note 140, at 44 (responding to Professor Kerr and arguing that the third party doctrine is arbitrary), *with* Tokson, *supra* note 38, at 581 (arguing that information provided only to automated systems does not result in a loss of privacy under the third party doctrine).

275 Smith v. Maryland, 442 U.S. 735, 741, 743 (1979).

276 Couch v. United States, 409 U.S. 322, 335-36 (1973).

277 Cal. Bankers Assn. v. Shultz, 416 U.S. 21, 52 (1974).

278 Whalen v. Roe, 429 U.S. 589, 602 (1977).

279 United States v. Miller, 425 U.S. 435, 442-43 (1976); *see also* United States v. Payner, 447 U.S. 727, 731-32 (1980) (criminal defendant had no standing to suppress documents illegally seized from a bank officer's briefcase because he had no privacy interest in them).

280 Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 338 (2011) (citing cases).

warrant.[281] By treating public exposure and third-party access to personal information as waivers of Fourth Amendment protections, modern doctrine offers a difficult path to erecting protections against government surveillance conducted by piecing together various public and private sector data with images posted online or captured in plain sight.

2. Digital Age

The Court has grappled for decades with the related question of whether—and the extent to which—government can use technology to enhance its ability to "see" what is arguably exposed to the public. It held in 1983 that there is no legitimate expectation of privacy in the interior of a car illuminated by a flashlight because "the use of artificial means to illuminate a darkened area simply does not constitute a search."[282] Three years later, it found that warrantless naked-eye aerial observation of a fenced-in backyard was not unreasonable under the Fourth Amendment as "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[283]

In 2001, however, the Court recognized emerging technologies' privacy implications when it decided that the use of thermal imaging technology to measure heat emanating from a home was a search because it amounted to "more than naked-eye surveillance" with "a device that is not in general public use."[284] As Justice Alito recently described it, *Kyllo v. United States*[285] was "a decision about the use of new technology."[286] Writing for the majority in *Florida v. Jardines*,[287] Justice Scalia similarly distinguished *Kyllo* as a case involving surveillance technology that allows law enforcement to learn details "that would previously have been unknowable *without physical intrusion*."[288] He reached the conclusion that a drug-sniffing police

---

281 *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); *see generally* Semitsu, *supra* note 280, at 338 n.186 (citing cases). *But see* Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007) (holding that a sender of electronic mail has a reasonable expectation of privacy in messages residing with an ISP), *vacated in part*, 532 F.3d 521 (6th Cir. 2008).

282 Texas v. Brown, 460 U.S. 730, 739-40 (1983) (plurality opinion); *cf.* United States v. Place, 462 U.S. 696, 707 (1983) (finding no Fourth Amendment barrier to the "*sui generis*" use of a drug-sniffing police dog).

283 California v. Ciraolo, 476 U.S. 207, 213-14 (1986).

284 Kyllo v. United States, 533 U.S. 27, 33, 40 (2001). As *Katz* itself arguably falls into this category, the pre-digital and digital distinction is not a hard and fast one; it is simply offered as a way of understanding how Fourth Amendment doctrine must adapt to technology.

285 533 U.S. 27 (2001).

286 Florida v. Jardines, 133 S. Ct. 1409, 1425 (2013) (Alito, J., dissenting). Chief Justice Roberts, along with Justices Kennedy and Breyer, joined the dissent. Justice Kagan suggested that *Kyllo* governed. *Id.* at 1419 (Kagan, J., concurring).

287 133 S. Ct. 1409 (2013).

288 *Id.* at 1417 (quoting *Kyllo*, 533 U.S. at 40) (internal quotation marks omitted).

dog deployed from the front porch of a home constituted a Fourth Amendment search despite "the antiquity" of forensic dogs as an investigative tool because there was no implicit license or invitation for the police to approach the home for the purpose of obtaining incriminating evidence inside.[289]

Earlier, in *City of Ontario v. Quon*,[290] the Court similarly highlighted the novelty of new technology as relevant to whether the user of a government-issued pager had a reasonable expectation of privacy in messages retained by the service provider. Sidestepping the Fourth Amendment question on the merits, Justice Kennedy cautioned that it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment," else it "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[291] He explained that modern judges are not "on so sure a ground" as the *Katz* Court was in relying on "its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth."[292] "Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior," he continued, and "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means . . . for self-expression, even self-identification," thus potentially "strengthen[ing] the case for an expectation of privacy."[293]

Two additional cases highlight the modern Court's struggle with fitting modern technologies within the existing Fourth Amendment rubric. In *United States v. Jones*,[294] the Court held that the warrantless installation of a global positioning system ("GPS") device to monitor the location of a person's car constituted a search because the police "physically occupied private property for the purpose of obtaining information."[295] Justice Scalia thus revived for the majority the old, property-based approach to the Fourth Amendment[296] instead of taking an arguably more obvious tactic: applying *United States v. Knotts*[297] for the proposition that there is "no reasonable expectation of privacy in [a driver's] movements from one place to anoth-

---

289 *Id.* at 1416-17.

290 130 S. Ct. 2619 (2010).

291 *Id.* at 2629-30.

292 *Id.* at 2629.

293 *Id.* at 2629-30. Only Justice Scalia declined to join in this sentiment, although he did acknowledge that "[a]pplying the Fourth Amendment to new technologies may sometimes be difficult." *Id.* at 2635 (Scalia, J., concurring in part and concurring in the judgment).

294 132 S. Ct. 945 (2012).

295 *Id.* at 949. In reaching its holding, the majority thus undermined the staying power of *Katz*'s reasonable-expectation-of-privacy formulation for what constitutes a Fourth Amendment search.

296 *Id.*

297 460 U.S. 276 (1983).

er."[298] Declaring *Katz* the *in*exclusive test, Justice Scalia confined it to "[s]ituations involving merely the transmission of electronic signals without trespass,"[299] while conceding that electronic surveillance "without an accompanying trespass" of a GPS device could amount "an unconstitutional invasion of privacy" in a future case.[300]

Justice Sotomayor[301]—and, separately, Justice Alito,[302] joined by Justices Ginsberg, Breyer, and Kagan—expressed concern that modern technology is eroding individuals' ability to be free of government monitoring. She wrote that "electronic or other novel modes of surveillance [can] generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations"—without any physical invasion of property.[303] The government, she added, can store and mine such data indefinitely.[304] Because modern electronic surveillance is cheap by comparison to traditional surveillance techniques, it "proceeds surreptitiously" and "evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[305] She referred to the Fourth Amendment's "goal to . . . prevent 'a too permeating police surveillance'"[306] and questioned the propriety of the third-party doctrine as "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," such as phone numbers, URLs visited, corresponding email addresses, "and the books, groceries, and medications they purchase" online.[307] Although some people might accept this diminution of privacy as a "tradeoff" for access to technology or simply "inevitable," she expressed "doubt that people would accept without complaint the warrantless disclo-

---

298 *Id.* at 281. Similarly, in *Florida v. Jardines*, 133 S. Ct. 1409, 1416 (2013), Justice Scalia utilized an implied license theory to find that the use of a drug-sniffing dog on a front porch of a home was a Fourth Amendment violation—rather than the established rule that "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." Kyllo v. United States, 533 U.S. 27, 31 (2001).

299 *Jones*, 132 S. Ct. at 953.

300 *Id.* at 954. Justice Powell similarly warned in his *Ciraolo* dissent that "[t]echnological advances have enabled police to see people's activities and associations, and to hear their conversations, without being in physical proximity." California v. Ciraolo, 476 U.S. 207, 218 (1986) (Powell, J., dissenting).

301 *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

302 *Id.* at 964 (Alito, J., concurring in the judgment).

303 *Id.* at 955 (Sotomayor, J., concurring) (citations omitted); *see also id.* at 962-94 (Alito, J., concurring in the judgment).

304 *Id.* at 955-56 (Sotomayor, J., concurring).

305 *Id.* at 956 (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)). FRT is even more probative than GPS tracking, as it can be immediately associated with a trove of online personal data, including browsing and buying habits and intimate communications with people who would not be identified with a GPS device.

306 *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

307 *Jones*, 132 S. Ct. at 957.

sure to the Government of a list of every Web site they had visited in the last week, or month, or year."[308]

For his part, Justice Alito focused on the problem of "long-term monitoring," agreeing in principle with the majority that "we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[309] Of course, he added, "it is almost impossible to think of late-18th-century situations" analogous to the capabilities of modern surveillance technology.[310] The majority's physical trespass theory, he explained, "would provide no protection" to "long-term monitoring . . . accomplished without committing a technical trespass,"[311] yet "[f]or such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[312] Justice Alito thus recognized that because "new devices" such as closed-circuit television video monitoring, automatic toll collection systems with recording technology, built-in GPS systems, and wireless tracking devices embedded in cell phones "permit the monitoring of a person's movements" in ways that were impossible before the digital age, traditional Fourth Amendment analysis is inapposite.[313]

Maryland v. King[314] is the most recent case in which the Supreme Court addressed the vexing intersection of technology and privacy under the Fourth Amendment. At a booking on an arrest for assault, the police took a DNA sample by applying a buccal swab to the inside of a suspect's cheek.[315] The DNA matched that of a rape victim taken six years earlier, leading to the arrestee's subsequent rape conviction.[316] The DNA matching occurred through the Combined DNA Index System ("CODIS"), which connects DNA data at the national, state, and local levels under FBI supervision.[317] On appeal, a Maryland court held that the cheek swab was an unreasonable search under the Fourth Amendment.[318] Reversing, Justice Kennedy wrote for the majority that a Fourth Amendment search occurred, but that it was reasonable and did not require a warrant.[319] For him, identifying an arrestee properly connotes "more than just" linking a name and social

---

308 *Id.*

309 *Id.* at 958 (Alito, J., concurring in the judgment) (alteration in original) (quoting *Jones*, 132 S. Ct. at 950 (majority opinion)) (internal quotation marks omitted).

310 *Id.*

311 *Id.* at 961.

312 *Id.* at 964.

313 *Jones*, 132 S. Ct. at 963.

314 133 S. Ct. 1958 (2013).

315 *Id.* at 1965.

316 *Id.*

317 *Id.* at 1968.

318 King v. State, 42 A.3d 549, 581 (Md. 2012), *rev'd*, 133 S. Ct. 1958.

319 *King*, 133 S. Ct. at 1965-66.

security number, but also "criminal history," aliases, photographs, and any other information that the police can obtain by "search[ing] the records already in their valid possession,"[320] such as "family ties, employment status and history, financial resources, reputation, character and mental condition, [and] length of residence in the community."[321] Justice Kennedy suggested that DNA is a mere relative of fingerprinting,[322] and that its value lies in allowing law enforcement "to make critical choices about how to proceed," ensuring that the accused remains available for trial, and helping protect the public from further harm—interests that, taken together, outweighed the arrestee's privacy interests in *King*.[323]

Although *King* would appear to narrow the availability of Fourth Amendment protections against invasive new technologies, three aspects of Justice Kennedy's decision distinguish DNA sampling from the dragnet-style surveillance of the general public which FRT makes possible. First, he emphasized that an arrestee's diminished expectations of privacy are distinguishable from those of "the public at large or a particular class of . . . law-abiding citizens."[324] Second, Justice Kennedy stressed that technology could progress to the point at which the Fourth Amendment balance would be struck in the arrestee's favor, such as if DNA showed a "predisposition for a particular disease or other hereditary factors not relevant to identity."[325] It is thus possible that the Court would condemn the warrantless use of FRT on law-abiding citizens for particularly invasive purposes. Third, a Maryland statute forbidding the use of DNA for anything other than identification "generally allay[ed] . . . privacy concerns" at issue in *King*.[326] In the absence of regulatory or statutory protections, the Court might grant the Constitution a greater role in protecting particular zones of privacy from unjustified government intrusion using FRT.

Justice Scalia's dissenting opinion, joined by Justices Ginsberg, Sotomayor, and Kagan, took issue with Justice Kennedy's characterization of King's DNA matching as mere identification.[327] For Justice Scalia, Justice Kennedy confused verification—the use of biometric data to confirm whether someone is whom he appears to be—with identification, which, properly understood, is more like "searching for evidence that [a person] has committed crimes unrelated to the crime of his arrest."[328] It "taxes the credulity of the credulous," Justice Scalia quipped, to assert that the DNA

320 *Id.* at 1971-72.

321 *Id.* at 1973 (quoting MD. R. 4-216(f)(1)(C)) (internal quotation marks omitted).

322 *Id.* at 1971-72.

323 *Id.* at 1972-73.

324 *Id.* at 1978.

325 *King*, 133 S. Ct. at 1979.

326 *Id.* at 1980 (second alteration in original) (quoting NASA v. Nelson, 131 S. Ct. 746, 750 (2011)) (citing MD. CODE ANN., PUB. SAFETY §§ 2-505(b)(1), 2-512(c) (LexisNexis 2011)).

327 *Id.* at 1980 (Scalia, J., dissenting).

328 *Id.* at 1982-83 (internal quotation marks omitted).

in *King* was not in fact used to solve crimes,[329] an aim "that ha[s] never been thought to justify a suspicionless search."[330] Justice Scalia likened the practice to so-called "general warrants" at the time of the Founding—those "not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application."[331] Justice Scalia also noted that the suspect's identity was already known when the state ran his DNA through the CODIS system long after he was arrested; the matching was thus performed in order to identify the DNA *sample* from the rape—not to verify identity.[332] What DNA offers that fingerprinting does not, he added, "is the ability to solve unsolved crimes, by matching old crime-scene evidence against the profiles of people whose identities are already known."[333] Justice Scalia warned that "[i]f one believes that DNA will 'identify' someone arrested for assault, he must believe that it will 'identify' someone arrested for a traffic offense."[334] His dissent in *King* is thus an acknowledgement that some constitutional limits must be placed on the uses of surveillance technologies that enable government to create new information by identifying correlations among otherwise disparate data points: "Perhaps the construction of . . . a genetic panopticon is wise," he wrote, "[b]ut I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection."[335]

B. *Anonymity and the First Amendment*

Separately, a line of First Amendment cases confirms that the privacy threat posed by technologies like FRT—the government's unfettered identification and monitoring of personal associations, speech, activities, and beliefs, for no justifiable purpose—is one of constitutional dimension. In fact, the Supreme Court has steadfastly protected anonymous speech.[336]

---

329 *Id.* at 1980.

330 *Id.* at 1983.

331 *King*, 133 S. Ct. at 1980-81.

332 *Id.* at 1984.

333 *Id.* at 1989.

334 *Id.*

335 *Id.*

336 As Justice Sotomayor suggested in *Jones*, the use of FRT and other technologies for identifying and tracking people may well give rise to a First Amendment claim in the appropriate case. *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). The aim of this Article is not to outline or further define whether a justiciable First Amendment case can be brought to limit the use of FRT for surveillance. Rather, it is to explore the intersection of First Amendment cases involving anonymous speech and Fourth Amendment privacy doctrine in the hopes of identifying a reinvigorated role for the Constitution in limiting the application of new technologies to public or third-party information for unprecedented surveillance. Arguably, the thesis has substantive due process implications. It also raises important questions regarding which branch of government is poised to enforce the constitutional values espoused here. These issues are beyond the scope of this Article. The Article more narrowly

The Court's repeated pronouncements that the First Amendment[337] safeguards the right of anonymous speech—that is, the right to distribute written materials without personal identification of the author—largely came about in response to government attempts to mandate disclosures in public writings.[338] In *Talley v. California,*[339] the Court struck down a Los Angeles ordinance restricting the distribution of a handbill "in any place under any circumstances, which does not have printed on the cover . . . the name and address of . . . [t]he person who printed, wrote, compiled or manufactured the same."[340] Finding that the law infringed on freedom of expression, the Court observed that "[a]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind" by enabling persecuted groups to criticize oppressive practices and other matters of public importance, particularly where the alternative may be not speaking at all.[341]

The *Talley* Court[342] relied on two cases that linked anonymous speech with the ability to freely associate in private. Both involved constitutional

---

concludes that the anonymity value embodied in First Amendment protections must be brought to bear in evolving Fourth Amendment doctrine as well as legislative and regulatory responses to the privacy threats posed by FRT and other technologies for surveillance, and it outlines substantive guidelines for consideration in these efforts.

337 U.S. CONST. amend. I (prohibiting the making of any "law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances").

338 McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."). While anonymous speech is protected, legislatures and courts have attempted to distinguish between "expressive" anonymity and anonymity used in the furtherance of criminal activity (or as a crime itself), referred to as "functional" anonymity. Though it is sometimes difficult to draw a bright line between the two, courts generally find that the latter does not warrant First Amendment protection. *See* Margot Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815, 817-18 (2013).

339 362 U.S. 60 (1960).

340 *Id.* at 60-61 (citing L.A., CAL., MUN. CODE § 28.06 (1960)).

341 *Id.* at 64-65; *see also* Shelton v. Tucker, 364 U.S. 479, 487-88 (1960) (striking down as overly broad state statute requiring public school teachers to file affidavits giving names of organizations to which they had belonged or contributed within the preceding five years as a condition of employment). *But see* New York *ex rel.* Bryant v. Zimmerman, 278 U.S. 63 (1928) (upholding state's enforcement of membership disclosure laws against Ku Klux Klan); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 465-66 (1958) (distinguishing *Bryant* on its facts). *See generally* Comment, *The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 70 YALE L.J. 1084, 1088 (1961) (discussing *Zimmerman* and other early Supreme Court cases bearing upon a constitutional right to anonymity).

342 *Talley*, 362 U.S. at 65.

challenges[343] to laws requiring members of the National Association for the Advancement of Colored People ("NAACP") to furnish government officials with its member lists. In *NAACP v. Alabama ex rel. Patterson*,[344] the lower court imposed a $100,000 civil contempt fine after the organization refused to comply with a court order requiring production of its lists.[345] The Supreme Court lifted the judgment and fine, holding that "immunity from state scrutiny of membership lists . . . is here so related to the right of the members to pursue their lawful private interests privately" as to be constitutionally protected on privacy and free association grounds.[346] Although "association" is not listed among the First Amendment's enumerated freedoms, the Court declared in *Talley* that "freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of . . . 'liberty.'"[347]

In *Bates v. City of Little Rock*,[348] the NAACP's records custodian was tried, convicted, and fined for refusing to comply with state ordinances requiring that membership lists "be public and subject to the inspection of any interested party at all reasonable business hours."[349] The organization claimed a right on the part of its members to participate in NAACP activities anonymously and "free from any restraints or interference from city or state officials"—a right that it felt "has been recognized as the basic right of every American citizen since the founding of this country."[350] The Supreme Court again struck down the ordinances, asserting that the freedom of speech, a free press, freedom of association, and a right to peaceably assemble are protected "from being stifled by [such] subtle governmental influence" as a requirement to divulge membership lists.[351]

---

343 Bates v. City of Little Rock, 361 U.S. 516, 517 (1960); *NAACP*, 357 U.S. at 451. The claims were brought under the Fourteenth Amendment's Due Process Clause, which makes the First Amendment applicable to the states. *See id.*

344 357 U.S. 449 (1958).

345 *Id.* at 452-54.

346 *Id.* at 462, 466. The *NAACP* Court took pains to note that the group had made "an uncontroverted showing that on past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility," but the Court found no compelling state interest in obtaining the lists. *Id.* at 462, 464.

347 *Id.* at 460. In *Griswold*, Justice Douglas construed associational freedom as falling within the First Amendment's "penumbra where privacy is protected from governmental intrusion" and otherwise "necessary in making the express guarantees fully meaningful." Griswold v. Connecticut, 381 U.S. 479, 483 (1965); *see also* Whalen v. Roe, 429 U.S. 589, 599 n.25 (1977) (quoting *Griswold*); Cal. Bankers Assn. v. Shultz, 416 U.S. 21, 78-79 (1974) (Powell, J., concurring) ("Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy.").

348 361 U.S. 516 (1960).

349 *Id.* at 518.

350 *Id.* at 520-21.

351 *Id.* at 523.

Over four decades later, the Court in *McIntyre v. Ohio Elections Commission* characterized anonymous speech as important to the preservation of personal privacy.[352] In *McIntyre,* the plaintiff distributed leaflets opposing a school superintendent's referendum which were anonymously attributed to "CONCERNED PARENTS AND TAX PAYERS."[353] The Ohio Election Commission fined the plaintiff for violating state laws banning the distribution of unsigned leaflets.[354] The U.S. Supreme Court reversed a lower court ruling upholding the ordinance, explaining that "an author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment"—even if "[t]he decision in favor of anonymity [is] motivated . . . merely by a desire to preserve as much of one's privacy as possible."[355] The Court extolled the virtues of anonymity as fostering "[g]reat works of literature . . . under assumed names," enabling groups to criticize the government without the threat of persecution, and "provid[ing] a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent."[356] As "core political speech," it concluded, "[n]o form of speech is entitled to greater constitutional protection."[357]

Justice Stevens went on in his majority opinion to tether anonymity to the purpose behind the Bill of Rights and the First Amendment: "to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society."[358] "Anonymity," he explained, "is a shield from the tyranny of the majority."[359] In a concurring opinion, Justice Thomas commented that the Founders' "practices and beliefs" on the subject "indicate[] that they believed the freedom of the press to include the right to author anonymous political articles and pamphlets."[360] "That most other Americans shared this understanding," he added, "is reflected in the Federalists' hasty retreat before the withering criticism of their assault on the liberty of the press."[361] Justice Scalia dissented, arguing that anonymity "facilitates wrong by eliminating accountability, which is ordinarily [its] very purpose."[362] To treat "all anonymous communication . . . in our society

---

352 514 U.S. 334, 342, 347 (1995).

353 *Id.* at 337 (internal quotation marks omitted).

354 *Id.* at 338.

355 *Id.* at 341-42.

356 *Id.*

357 *Id.* at 347.

358 *McIntyre*, 514 U.S. at 357.

359 *Id.* (citing J. S. MILL, ON LIBERTY AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT 1, 3-4 (R. B. McCallum ed., 1948)).

360 *Id.* at 360, 364 (Thomas, J., concurring in the judgment).

361 *Id.* at 364.

362 *Id.* at 385 (Scalia, J., dissenting). Justice Scalia flatly rejected the notion that "a 'right to anonymity' is such a prominent value in our constitutional system that even protection of the electoral process cannot be purchased at its expense." *Id.* at 379. In his view, "[a]nonymity can still be enjoyed by

[as] traditionally sacrosanct," he continued, "seems to me a distortion of the past that will lead to a coarsening of the future."[363]

In *Watchtower Bible & Tract Society of New York, Inc. v. Village of Stratton*,[364] the Court struck down an ordinance requiring permits for door-to-door canvassing as a prior restraint on speech but also because the law vitiated the possibility of anonymous speech.[365] It characterized the permit requirement as "result[ing] in a surrender of . . . anonymity"—even where "circulators revealed their physical identities"—because "strangers to the resident certainly maintain their anonymity."[366] The Court was thus unmoved by the fact that speakers who ring doorbells necessarily make themselves physically known to their audience, thus revealing themselves to some extent. For the Court, it was the *recognition* that occurs when a name on a permit is connected to a face which triggered the Constitution's protection of anonymity.

Most recently, a fractured plurality in *Doe v. Reed*[367] upheld a state law compelling public disclosure of the identities of referendum petition signatories while squarely acknowledging the vitality of a First Amendment right to anonymous speech.[368] Significantly, all but one Justice recognized that the government's ability to correlate identifying information with online data created a First Amendment hazard of unprecedented dimension. Writing for the majority, Chief Justice Roberts found that an individual's expression of a political view through a signature on a referendum petition implicated a First Amendment right.[369] The Court nonetheless held that the state's interest in preserving the integrity of the electoral process and informing the public about who supports a petition justified the burdens of compelled disclosure.[370] Justice Roberts made a point of deeming "significant" the plaintiffs' argument that, "once on the Internet," their names and addresses could be matched with other publicly available information about them "in what will effectively become a blueprint for harassment and intim-

---

those who require it, without utterly destroying useful disclosure laws." *Id.* at 380. Justice Scalia's answer is to require a showing of a "'reasonable probability' that the compelled disclosure would result in 'threats, harassment, or reprisals from either Government officials or private parties,'" consistent with the disclosure requirements of the Federal Election Campaign Act. *Id.* at 379 (quoting Buckley v. Valeo, 424 U.S. 1, 74 (1976) (per curiam)).

363 *Id.* at 379.

364 536 U.S. 150 (2002).

365 *See* Berger v. City of Seattle, 569 F.3d 1029, 1037-38 (9th Cir. 2009) (discussing *Watchtower Bible & Tract Soc'y*).

366 *Watchtower Bible & Tract Soc'y*, 536 U.S. at 166-67.

367 130 S. Ct. 2811 (2010).

368 *Id.* at 2815. Chief Justice Roberts wrote the majority opinion. Justices Breyer, Alito, and Sotomayor each wrote separately, while Justices Stevens and Scalia wrote opinions concurring in the judgment. Justice Thomas dissented.

369 *Id.* at 2817.

370 *Id.* at 2819.

idation."[371] Because the majority only considered the facial challenge to the law, Justice Roberts found the burdens imposed by "typical referendum petitions" unlike those that the plaintiffs feared.[372]

Justice Alito wrote separately to emphasize that government access to personal data online gave rise to a strong as-applied challenge based on the "individual . . . right to privacy of belief and association."[373] He considered "breathtaking" the implications of the state's argument that it has an interest in providing information to the public about supporters of a referendum petition; if true, "the State would be free to require petition signers to disclose all kinds of demographic information, including the signer's race, religion, political affiliation, sexual orientation, ethnic background, and interest-group memberships."[374] Justice Alito added that the posting of names and addresses online could allow "anyone with access to a computer [to] compile a wealth of information about all of those persons," with vast potential for use in harassment.[375] Justice Thomas dissented on similar grounds, asserting that he would sustain a facial challenge precisely because "[t]he advent of the Internet enables rapid dissemination of the information needed to threaten or harass every referendum signer," thus "chill[ing] protected First Amendment activity."[376] Concurring separately, Justice Scalia stood alone in his complete rejection of First Amendment protections for anonymous speech.[377]

---

371 *Id.* at 2820.

372 *Id.* at 2821.

373 *Doe*, 130 S. Ct. at 2824 (Alito, J., concurring).

374 *Id.*

375 *Id.* at 2825. Justice Sotomayor wrote a concurring opinion in which Justices Stevens and Ginsburg joined. She suggested "the State's decision to make accessible what [citizens] voluntarily place in the public sphere should not deter them from engaging in the expressive act of petition signing," and she distinguished *NAACP v. Alabama ex rel. Patterson* on the grounds that case-specific relief is appropriate if there is a reasonable probability of harassment. *See id.* at 2828-29 (Sotomayor, J., concurring) (citing NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958)). In a separate concurrence in which Justice Breyer joined, Justice Stevens emphasized that, unlike in *McIntyre*, the law "does not . . . require that any person signing a petition disclose or say anything at all." *Id.* at 2829 (Stevens, J., concurring) (citing McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 345 (1995)). Justice Sotomayor's suggestion that First Amendment protections for privacy of belief or associations are waived upon public disclosure of one's identity seems at odds with her critique of the Fourth Amendment's third party doctrine. *See supra* notes 301-308 and accompanying text (discussing Justice Sotomayor's concurrence in *United States v. Jones*, 132 S. Ct. 945 (2012)).

376 *Doe*, 130 S. Ct. at 2845 (Thomas, J., dissenting) (quoting Citizens United v. Fed. Election Comm'n, 130 S. Ct. 876, 982 (2010) (Thomas, J., concurring in part and dissenting in part)) (internal quotation marks omitted).

377 Justice Scalia equated the signing of a referendum with acting as a legislator—not a voter; "when the people exercised legislative power directly, they did so not anonymously, but openly in town hall meetings." *Id.* at 2834 (Scalia, J., concurring in the judgment). He also characterized the case as claiming that public disclosure of signatories' identifying information "violates their First Amendment right to anonymity," and suggested that "[t]oday's opinion acknowledges such a right." *Id.* at 2832.

When considered in conjunction with the digital-age Fourth Amendment cases, *Doe* is remarkable in its recognition of the pressures that modern technology puts on the viability of existing constitutional doctrine relating to individual privacy. Although *Jones* addressed GPS monitoring under the Fourth Amendment, Justice Sotomayor invoked the First Amendment to emphasize that "[a]wareness that the Government may be watching chills associational and expressive freedoms," and that "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[378] When inexpensive technology is paired with massive amounts of readily accessible personal information and "unfettered" government discretion to track individual citizens, she explained, democracy itself suffers.[379] Although pre-digital-age Fourth Amendment case law appears to paint FRT surveillance into a doctrinal corner, in the right case the Supreme Court may well find constitutional limits on surveillance conducted with cutting-edge technology like FRT and publicly available data. The next Part offers guidelines derived from the Court's Fourth and First Amendment jurisprudence which courts and legislators should bear in mind in crafting legal limits on surveillance through technologies like FRT.[380]

III. RECLAIMING THE CONSTITUTION'S ROLE IN PROTECTING ANONYMITY

To address the privacy threats posed by modern technology, scholars have argued for recognition of a wholesale constitutional right to anonymity, as well as robust enforcement of First Amendment protections of that

---

Justice Stevens disagreed, stating that "[t]he right . . . is the right to speak, not the right . . . to speak anonymously." *Id.* at 2831 n.4 (Stevens, J., concurring in part and concurring in the judgment).

378 United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

379 *See id.*

380 Note that there would likely be a formidable Article III justiciability problem to a First Amendment challenge to the government's use of third party information and technology for its own surveillance. In *California Bankers*, the Court found unripe the American Civil Liberties Union's claim that the banks' record keeping requirements violated the First Amendment as they "could *possibly* be used to obtain the identities of its members and contributors through the examination of the organization's bank records." Cal. Bankers Assn. v. Shultz, 416 U.S. 21, 55-56 (1974) (emphasis added). In *Laird v. Tatum*, the Court similarly found no standing to challenge the Army's practice of collecting and storing "information about public activities that were thought to have at least some potential for civil disorder." 408 U.S. 1, 6 (1972). The Court found that the plaintiff lacked standing to press a claim that "the exercise of his First Amendment rights is being chilled by the mere existence, without more, of a governmental investigative and data-gathering activity that is alleged to be broader in scope than is reasonably necessary for the accomplishment of a valid governmental purpose." *Id.* at 10. In dissent, Justice Douglas argued that "[t]here is . . . no law authorizing surveillance over civilians, which in this case the Pentagon concededly had undertaken," yet "[o]ne can search the Constitution in vain for any such authority." *Id.* at 16 (Douglas, J., dissenting).

right in the face of widespread technological surveillance of the public.[381] A plethora of scholarship has also arisen in response to the problems of new technologies under existing Fourth Amendment doctrine. Like Justice Sotomayor in *Jones,* some commenters have called for the end of the third party doctrine,[382] reconsideration of the case law truncating the Fourth Amendment's reach in public spaces,[383] and adoption of new theories for understanding the Fourth Amendment guarantee altogether.[384]

This Part seeks to reclaim the Constitution's relevance in protecting anonymity in the digital age by identifying points at which the Supreme Court's First Amendment cases on anonymity and its modern Fourth Amendment jurisprudence intersect. FRT and related technologies employ big data to make correlations that help predict the future in ways that were impossible only a few years ago.[385] It is through such correlations that FRT enables users to recognize—versus merely see—a subject, and from that data erect a comprehensive portrait of that person's past, present, and future life. At least three guidelines can be inferred from the Court's First and Fourth Amendment cases which courts, legislators, and regulators should take into account in responding to the privacy challenges posed by such technologies' unlimited access to the whereabouts, activities, interests, associations, and beliefs of virtually any member of society. First, the intend-

---

381 Slobogin, *supra* note 23, at 217 (observing that "we all possess a 'right to anonymity,' even when in public," under the Fourth Amendment); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 749 (2008) (arguing that "the First Amendment right to freedom of association provides the strongest basis for regulating relational surveillance" and identifying "suggestive principles from Fourth Amendment doctrine about how surveillance regulation must respond to technological change"); Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 FLA. L. REV. 1, 3-4 (2007) (providing "a comprehensive assessment of the First Amendment issues related to the networking of public places" and categorizing the speech issues into six basic clusters); *see* Lynch, *supra* note 205, at 235 (arguing that free speech under the First Amendment should be expanded "to encompass a speaker's right to choose a private audience").

382 *Compare* Henderson, *supra* note 140, at 45, *with* Kerr, *supra* note 274, at 566 (taking different approaches to the third party doctrine).

383 *See, e.g.*, Slobogin, *supra* note 23, at 312-13 ("Whether framed in the Court's language—in terms of expectations of privacy society is prepared to recognize as reasonable—or in mine—in terms of a right to anonymity that protects against unnecessary government scrutiny—that threshold is crossed when government trains cameras on its citizens, because of the panoptic atmosphere such surveillance creates . . . ."); *id.* at 270-71 & n.255 (citing scholarship "to show that the Court's public exposure/assumption of risk approach to the Fourth Amendment is misguided").

384 *See, e.g.*, Citron & Gray, *supra* note 185, at 270 (arguing that "continuous and indiscriminate surveillance . . . is damaging because it violates reasonable expectations of *quantitative* privacy, by which we mean privacy interests in large aggregations of information that are independent from particular interests in constituent parts of that whole"); Kerr, *supra* note 125, at 313 (discussing "mosaic" theory of Fourth Amendment); Slobogin, *supra* note 23, at 258-67 (arguing that a right to anonymity additionally derives from a right to travel under the Due Process Clause and from a general right to privacy in the penumbras of the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments).

385 MAYER-SCHÖNBERGER & CUKIER, *supra* note 11, at 52-53.

ed use of technologically derived data should be treated as a significant factor in assessing the proper constitutional, statutory, and regulatory scope of government activity that has the potential to expose an individual's privacy to scrutiny. Second, and accordingly, the law should place boundaries around the ability of government to match faceprints with other data points for purposes other than verification of an individual's known identity. Third, courts and lawmakers should keep in mind that legislative protection of an individual's ability to invoke anonymity—through conspicuous and mandatory opt-out provisions for web tracking, for example—is constitutionally prudent, if not necessary.

A. *Recognition Through Correlation*

As the First Amendment cases indicate, anonymity implies a freedom from being recognized—versus just being seen. In spite of surveillance technology's reach, people still expect to mostly avoid recognition while going about their daily routines. As technology changes the way information is collected and used, however, the viability of that assumption is eroding. Big data "is about predictions."[386] It operates by "applying math to huge quantities of data in order to infer probabilities," such as "the likelihood that an email message is spam; that the typed letters 'teh' are supposed to be 'the'; that the trajectory and velocity of a person jay-walking mean he'll make it across the street in time" to avoid a driverless car; and even that a person is a criminal "before one actually commits a crime."[387] It is the linkage of a faceprint with a name, a Facebook tag, a driving record, and real-time footage from an airport or ATM camera—not just the collection of the faceprint itself—which remains unaccounted for in prevailing Fourth Amendment doctrine. The Supreme Court has construed the First Amendment as protecting speech that enables *recognition* by the government. If extended to the Fourth Amendment context, this idea would help modernize what it means to perform a search with technology which does not result in a physical trespass.

In both the First and Fourth Amendment arenas, the Court has treated "the right . . . to pursue . . . lawful private interests privately" as constitutionally protected from government interference.[388] Yet it has never suggested that the public disclosure of one's face is itself an act of constitutional dimension. In addressing anonymity, the Court has instead drawn a distinction between mere observance of "physical identities" and recogni-

---

386 *Id.* at 11.

387 *Id.* at 12.

388 NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 466 (1958); *see also* Boyd v. United States, 116 U.S. 616, 630 (1886) (framing the Fourth Amendment question as implicating the "indefeasible right of personal security, personal liberty and private property").

tion.[389] A stranger knocking on a door might remain anonymous even though his face is visible. A "surrender of . . . anonymity" takes place when the face is linked to other identifying information, such as a name on a pamphlet.[390] Chief Justice Roberts extended this principle to modern technology when he emphasized in *Doe v. Reed* that "once on the Internet" names and addresses contained in referendum petitions could be matched with other data "in what will effectively become a blueprint for harassment and intimidation."[391] Similarly, Justice Alito deemed "breathtaking" the implications of the government's ability to match referendum petition information with other online data.[392] And Justice Thomas associated chilled speech with the "advent of the Internet" and "rapid dissemination" of personal information that may be used "to threaten or harass every referendum signer."[393] Forcing individuals to enable others to *recognize* them through public writings is anathema to First Amendment freedoms of speech and association.[394]

Standing alone, a photo is likewise of limited investigative utility. "With big data," its value "is now in secondary uses."[395] FRT works by "electronically matching aspects of each person's appearance against biometric or other databases."[396] Using a single image, government can "probe our lives after the fact" by, for example, "figuring out what specific medical or social problem led . . . to a certain source of help."[397] It does this by drawing correlations between a faceprint and other information contained in databases or online. In his concurring opinion in *Whalen v. Roe*,[398] Justice Brennan was presciently "troubl[ed]" by "the central computer storage of the data . . . collected" back in 1977 because it allowed government to manipulate information in ways that could harm privacy interests—even though the Fourth Amendment did not shield the information itself from

---

389 Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166-67 (2002).

390 *Id.* at 166.

391 Doe v. Reed, 130 S. Ct. 2811, 2820 (2010); *see also* Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182, 198-200 (1999) (invaliding Colorado law requiring identification badges when soliciting signatures for ballot initiatives as it "forces circulators to reveal their identities at the same time they deliver their political message," thus exposing them to "'heat of the moment' harassment"—"at the precise moment when the circulator's interest in anonymity is greatest" (quoting Am. Constitutional Law Found., Inc. v. Meyer, 120 F.3d 1092, 1102 (10th Cir. 1997), *aff'd sub nom.* Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182) (internal quotation marks omitted)).

392 *Doe*, 130 S. Ct. at 2824 (Alito, J., concurring).

393 *Id.* at 2845 (Thomas, J., dissenting) (quoting Citizens United v. Fed. Election Comm'n, 130 S. Ct. 876, 982 (2010) (Thomas, J., concurring in part and dissenting in part)) (internal quotation marks omitted).

394 *Id.* at 2843.

395 MAYER-SCHÖNBERGER & CUKIER, *supra* note 11, at 153.

396 Blitz, *supra* note 148, at 1356.

397 *Id.* at 1358.

398 429 U.S. 589 (1977).

government scrutiny in that case.[399] In his view, "[t]he central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information."[400] "[F]uture developments," he suggested, might one day "demonstrate the necessity of some curb on such technology."[401] In *United States v. Knotts,* the Court similarly acknowledged that, if "dragnet type law enforcement practices" such as twenty-four-hour surveillance "without judicial knowledge or supervision . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[402]

That time has come. Technology has progressed to the point at which FRT and big data can be used to make predictions about people's behavior. This occurs through the analysis of "the statistical relationship between two data values."[403] "[I]f *A* often takes place together with *B*," law enforcement might conclude that "we need to watch out for *B* to predict that *A* will happen."[404] A correlation between the two data points assumes that if one data value changes, the other is likely to change as well.[405] In the foregoing example, *B* operates as a proxy for what is probably happening with *A,* even if *A*'s future activity cannot be directly observed.[406] Target stores' marketing toward mothers-to-be provides an impactful example of the power of big-data correlations in the private sector. By reviewing the shopping histories of women with baby registries, Target identified products that correlate with pregnancy and calculated "pregnancy prediction" scores for new customers; it then sent customers coupons tailored to individual due dates that it estimated with astonishing accuracy.[407] Similarly, although a faceprint algorithm in and of itself is just a numerical record of something that has already been made public, the *correlation* of that data with other information for predictive surveillance is altogether different. "The data may not even explicitly seem like personal information, but with big-data processes it can easily be traced back to the individual it refers to. Or intimate details about a person's life can be deduced."[408]

The Supreme Court's view that there is no reasonable expectation of privacy in things made public has thus been criticized for narrowly defining

---

399 *Id.* at 606-07 (Brennan, J., concurring).

400 *Id.* at 607.

401 *Id.*

402 460 U.S. 276, 283-85 (1983) (internal quotation marks omitted) (holding that beeper signals did not invade reasonable expectations of privacy).

403 MAYER-SCHÖNBERGER & CUKIER, *supra* note 11, at 52.

404 *Id.* at 53.

405 *Id.*

406 *Id.*

407 *Id.* at 57-58 (internal quotation marks omitted).

408 *Id.* at 152.

privacy as mere secrecy.[409] Correlating an image with other data contained in a database is more intrusive than mere visual surveillance. People do not expect that many passersby recognize their faces, let alone associate them with Internet behavior or travel patterns.[410] Even if the gathering of a faceprint from a public closed-circuit camera is unobjectionable, its correlation with other big data produces new surveillance information that the subject did not knowingly convey.

The First Amendment anonymity cases indicate that the action of correlating FRT data with other information for purposes of identifying an otherwise anonymous person therefore should trigger the same constitutional scrutiny that applies to other means of surveillance such as the GPS device in *Jones*.[411] Whether the government retrieves the requisite image through a classic physical invasion of property should not determine whether the correlation process is constitutionally confined. Nor should the public or third-party nature of the data collected undermine the Constitution's role in protecting against the use of such data for omnipresent government monitoring. Instead, as the Court implied in *Jardines*,[412] new technology should be afforded distinct modes of Fourth Amendment analysis. The action of correlating numerical faceprints with other data amounts to "more than naked-eye surveillance of a home" with "a device that is not in general public use" under *Kyllo*'s formulation.[413] As Justice Sotomayor explained in *Jones,* modern methods of government monitoring rely on data mining and storage, "proceed[] surreptitiously" and cheaply, and "evade[] the ordinary checks that constrain abusive law enforcement practices."[414] Technology has enabled the government to "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[415] This novel use of bits of data defies what Justice Alito called "society's expectation . . . that law enforcement agents and others would not—and indeed, in

---

409 SOLOVE, *supra* note 14, at 23 (discussing theorists); *see also* Gutterman, *supra* note 103, at 665-66 (critiquing the *Katz* formulation as "too dependent upon a finding of objective measures used to protect privacy" and "thereby a risk-assumption theory" of the Fourth Amendment).

410 If an individual controls the database used for matching—such as a Facebook account—there may be an argument that the government's probing of such data constitutes an unreasonable search of that person's "effects" under the Fourth Amendment. *But see, e.g.*, United States v. Gabel, No. 10-60168, 2010 WL 3927697, at *6-7 (S.D. Fla. Sept. 16, 2010) (rejecting argument that subject had a reasonable expectation that only users logging onto a network in a usual manner would see his information, and that law enforcement's use of enhanced technologies for searching violated the Fourth Amendment), *aff'd*, 470 F. App'x 853 (11th Cir. 2012).

411 *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 89-90 (1995).

412 *See supra* notes 287-289 and accompanying text.

413 *See* Kyllo v. United States, 533 U.S. 27, 33, 40 (2001).

414 United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

415 *Id.* at 955.

the main, simply could not—secretly monitor and catalogue [one's] every single movement" over a long period of time.[416]

B. *Limited Use of Data*

The Court's First Amendment approach to anonymity and its Fourth Amendment treatment of technology in the digital age further suggest that, doctrinally, the collection of data might be constitutional for one use but not for another. FRT analysis allows users to make predictions about a subject's behavior which can be tremendously useful in preventing crime but also hugely problematic in terms of personal privacy and autonomy. Even if the collection of personal data through public interfaces is lawful, the Constitution could confine the extent to which law enforcement can employ new technologies for predictive surveillance.

In their opinions in *Doe,* Justices Alito and Thomas suggested that there is a meaningful distinction under the First Amendment between using personal information contained on referendum petitions for verification and using the information for other purposes.[417] Unlike verification, identification links a face with a wealth of personal information about an individual from the Internet and other public and private sources, such as birth date and place, medical data, affiliated friends and organizations, and criminal history. This data can be put toward law enforcement aims that go well beyond verification that a person is in fact whom he claims to be. Justice Scalia emphasized as much in his *Maryland v. King* dissent, when he assailed the majority for characterizing the government's use of the suspect's DNA as unrelated to crime solving.[418] He explained in great detail how the police employed the DNA sample to "solve unsolved crimes, by matching old crime-scene evidence against the profiles of people whose identities [were] already known."[419] In *Jardines,* as well, Justice Scalia suggested that the intended use of a technology (such as a drug-sniffing dog) is an important element of the Fourth Amendment analysis.[420] He distinguished between licensed and unlicensed entries into a curtilage (e.g., knocking on a door versus arriving with a bloodhound or a metal detector) and suggested that "[a]n invitation to engage in canine forensic investigation assuredly does not inhere in the very act of hanging a knocker."[421] As to the reasonableness

---

416 *Id.* at 964 (Alito, J., concurring in the judgment).

417 Doe v. Reed, 130 S. Ct. 2811, 2826 (2010) (Alito, J., concurring) (observing that the state laws suggest that signatory information should be confidential except for verification); *id.* at 2847 (Thomas, J., dissenting) (observing that the rules allowing for review of the secretary of state's verification decisions were not in question).

418 133 S. Ct. 1958, 1980 (2013) (Scalia, J., dissenting).

419 *Id.* at 1989.

420 133 S. Ct. 1409, 1416 (2013).

421 *Id.*

of a search, Justice Scalia similarly observed that it "depends upon whether the officers had an implied license to enter the porch, which in turn depends upon the purpose for which they entered."[422]

If—unlike the DNA in *King*—faceprints were used for surveillance of common citizens, a majority of the Court might find that the Fourth Amendment applies to limit the use of such data for secondary purposes that include identification versus mere verification of identity. The First Amendment anonymity cases provide insight into how courts might determine whether a secondary use of faceprint data is constitutional. In *McIntyre v. Ohio Elections Commission*, for example, the Court credited the state's interest in preventing fraud and libel during elections "when false statements, if credited, may have serious adverse consequences for the public at large," but found it insufficient under the "exacting scrutiny" applicable to core political speech.[423] Under that standard, "[t]he simple interest in providing voters with additional relevant information" did not justify the anonymity ban, which did little to help voters evaluate the pamphlet's message.[424]

By the same token, "[t]he FBI shouldn't be in the business of monitoring demonstrations unless it has a cause, a tip, a reason."[425] In order to develop meaningful constitutional distinctions between the various possible uses of facial data collected in the public sphere, the Court's identification of the government's rationale for collecting personal information in the First Amendment cases could be extrapolated to the Fourth Amendment context. In other words, if anonymity warrants constitutional protection under the First Amendment, some requisite showing should be made before the government can perform a matching that results in monitoring of an individual's activity as a matter of Fourth Amendment law, as well.[426] Lower courts have held that before the government can utilize fingerprint evidence gathered from the general public, it must demonstrate probable cause. If the government cannot show probable cause, it must at least show an articulable suspicion to believe that the person committed a criminal offense and that fingerprinting will establish or negate the person's connection to the offense.[427] FRT should be treated no differently.[428] Whether fash-

---

422 *Id.* at 1417.

423 514 U.S. 334, 347, 349 (1995) (internal quotation marks omitted).

424 *Id.* at 348-49.

425 Spencer, *supra* note 157 (quoting Gregory Nojeim, senior counsel at the Center for Democracy and Technology).

426 This factor, of course, raises its own host of issues—such as what anonymity means for purposes of evaluating levels of Fourth Amendment scrutiny and protection—which is beyond the scope of this paper.

427 *See* Hayes v. Florida, 470 U.S. 811, 813-18 (1985) ("There is . . . support in our cases for the view that the Fourth Amendment would permit seizures for the purpose of fingerprinting, if there is reasonable suspicion that the suspect has committed a criminal act, if there is a reasonable basis for believing that fingerprinting will establish or negate the suspect's connection with that crime, and if the

ioned as probable cause, reasonable suspicion, or something else, First Amendment doctrine suggests that the government should have to justify its correlation of FRT data with other information to form a working profile of citizens who otherwise abide by the law.[429]

C. *The Importance of Choice*

With the exception of *Doe,* an important distinguishing feature of the First Amendment anonymity cases is the involvement of legislative attempts to coerce the disclosure of personal identities. FRT presents a particularly difficult problem under prevailing constitutional law because most faces are routinely exposed in public. No domestic law requires that a person's facial features be unobstructed while she maneuvers about in public places so that the government can use them for identification purposes. Her visage is there for the government's taking. Technology has thus become deterministic of personal privacy today. Yet there is no reciprocal power on the part of individuals to direct how technology will evolve in relationship

---

procedure is carried out with dispatch. Of course, neither reasonable suspicion nor probable cause would suffice to permit the officers to make a warrantless entry into a person's house for the purpose of obtaining fingerprint identification." (citation omitted)); *cf.* Maryland v. King, 133 S. Ct. 1958, 1987 (2013) (Scalia, J., dissenting) (observing that "our cases provide no ready answer to th[e] question" of whether taking a person's fingerprints amounts to a Fourth Amendment search); Davis v. Mississippi, 394 U.S. 721, 728 (1969) ("We have no occasion in this case . . . to determine whether the requirements of the Fourth Amendment could be met by narrowly circumscribed procedures for obtaining, during the course of a criminal investigation, the fingerprints of individuals for whom there is no probable cause to arrest."). By contrast, courts have found that routine "booking" procedures may require fingerprint identification, regardless of whether investigation of the crime involves fingerprint evidence. *See, e.g.*, Napolitano v. United States, 340 F.2d 313, 314 (1st Cir. 1965) ("Taking of fingerprints [prior to bail] is universally standard procedure, and no violation of constitutional rights."); Smith v. United States, 324 F.2d 879, 882 (D.C. Cir. 1963) ("[I]t is elementary that a person in lawful custody may be required to submit to . . . fingerprinting . . . as part of routine identification processes.").

428 *See, e.g.*, Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1057-59 (Colo. 2002) (en banc) (applying the Supreme Court's recognition of a First Amendment interest in anonymity to a search warrant issued to a third party and holding that a warrant to obtain information about an individual's purchases from a bookseller could not be enforced without a heightened showing of the need for customers' book purchase records). Other courts have held that the privacy or anonymity interest of a party seeking to prevent a subpoena to a third party weakens if the party made disclosures to that third party in exchange for a service. *E.g.*, Hause v. Commonwealth, 83 S.W.3d 1, 12 (Ky. Ct. App. 2001) (upholding a warrant for subscriber records from an ISP because he had knowingly revealed his identity to the ISP, whose employees had access to that information).

429 *Cf.* MAYER-SCHÖNBERGER & CUKIER, *supra* note 11, at 176 (recommending that governments be required (1) to disclose their data and algorithms to the public, (2) to have algorithms certified by third parties prior to use in making predictions, and (3) to specify concrete ways in which individuals can disprove predictions made through big data correlations); Lee Tien, *Privacy, Technology and Data Mining*, 30 OHIO N.U. L. REV. 389, 405 (2004) (arguing that the lack of particularized suspicion to run a data search amounts to a violation of the Fourth Amendment).

to their privacy interests or even to opt out of its implications for their daily lives.

The First Amendment anonymity cases and Fourth Amendment doctrine assume that a person possesses the discretion to take steps to protect communications or other effects from governmental intrusion—that is, by keeping personal information private. In the First Amendment context, the Court has upheld private individuals' ability to choose to keep their identities anonymous in some respect. Indeed, the fact that the *McIntyre* plaintiff simultaneously disclosed her identity in other pamphlets was irrelevant to the Court's analysis and ultimate conclusion that her choice to remain anonymous was protected by the First Amendment.[430] In the Fourth Amendment arena, disclosure operates as a waiver of sorts, but the Court has taken pains to identify how the subject of police inquiry could have effectively invoked constitutional protections by keeping information private. In both contexts, the underlying assumption supporting the Court's analyses of the constitutional guarantee at issue is that citizens have a choice and—caveat emptor—if they choose public disclosure, the Constitution cannot save them from the consequences of that choice.

Facebook's FRT features are active by default.[431] It takes six clicks to reach a disclosure that Facebook uses FRT.[432] Apple's iPhoto does not have an opt-out function at all.[433] Currently, there are no laws requiring private entities to provide individuals with notice that they are collecting personal data using FRT, how long that data will be stored, whether and how it will be shared, or how it will be used.[434] Other countries have regulations that give Internet users control over their own data.[435] In the United States, however, private companies are free to sell, trade, and profit from individuals' biometric information. Private companies can also disclose individuals' data to government authorities without their consent.[436]

---

430 *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

431 Blue, *supra* note 47.

432 Ian Duncan, *Senator Questions Facebook Exec About Facial-Recognition Feature*, L.A. TIMES (July 18, 2012), http://articles.latimes.com/2012/jul/18/business/la-fi-senate-facebook-20120719.

433 jhon jabir, *How Facebook's Face Recognition Challenges Privacy*, SEETECHNO.COM (July 18, 2012), http://seetechno.com/how-facebooks-face-recognition-challenges-privacy/.

434 Blue, *supra* note 47.

435 *See generally Protection of Personal Data*, EUR. COMM'N, http://ec.europa.eu/justice/data-protection/ (last visited Nov. 24, 2013).

436 *See* Anita Ramasastry, *Lost in Translation?: Data Mining, National Security and the "Adverse Inference" Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 758 (2006) ("Since September 11, 2001, the federal government has tried to connect more 'dots' (data points) to prevent terrorism—by piecing together pieces of information and data to uncover possible plots and patterns. As part of this effort, the Executive Branch has introduced various proposals to 'mine' private sector commercial databases and public records (as well as public databases) for information on everything from consumer addresses to financial and credit profiles. Such information, when fed into computers and analyzed, is meant to help the U.S. government predict who might be involved in terrorist activity.").

Fourth and First Amendment law is remarkably consistent in its deference to the subject's *choice* to remain anonymous or put information into the public domain. If people protect their privacy, the Constitution protects it too. In modern times, the problem with this tautology is that the concept of choice implies that there is more than one meaningful option. With FRT and other emerging technologies, there is no mechanism for opting out of the various sources that are amalgamated into what amounts to surveillance. The theory behind the Fourth Amendment doctrines that lift its protections for information disclosed publicly or to third parties is thus unsustainable.

Accordingly, the recognition of anonymity as a constitutional value that warrants protection under the First and Fourth Amendments may require "numerous safeguards" in place for forestalling "indiscriminate disclosure," as Justice Brennan suggested in *Whalen*.[437] In his words, whether sophisticated storage and matching technology "amount[s] to a deprivation of constitutionally protected privacy interests" might depend in part on congressional or regulatory protections put in place to forbid the government's use of big data for arbitrary monitoring of the populace without individuals' consent.[438] This will not be easy. Choosing to "opt out" of Google's tracking technologies itself leaves a trace, and technology exists to "re-identify" people whose personal identifiers, such as name, address, credit card information, birth date, and social security number had been removed from a dataset.[439] But constitutional limits on the government's ability to work around individuals' attempts to protect their privacy would be an important step toward rescuing the constitutional value of anonymity before FRT and big data are used to do more than simply predict who may commit crimes—i.e., to punish people for future acts.[440]

---

437 Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan, J. concurring).

438 *Id.*; *see also* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment) (citing Kerr, *supra* note 125, at 805-06). One option is to have a comprehensive privacy law incorporating informed consent requirements, like many European countries have, with a "privacy commissioner" responsible for addressing technological developments in a regulatory environment. Freishtat, *supra* note 160. This would allow for different responses to different FRT applications, perhaps requiring social networks to be more transparent and to enable users to easily switch data to competitors. James Temple, *Facial Recognition Software's Privacy Concerns*, SFGate.com (June 20, 2012, 4:00 AM), http://www.sfgate.com/business/article/Facial-recognition-software-s-privacy-concerns-3645779.php.

439 MAYER-SCHÖNBERGER & CUKIER, *supra* note 11, at 154-55. These authors anticipate a shift in regulatory frameworks away from consent and toward accountability for the uses of data. *Id.* at 173.

440 *Id.* at 158-59. This would be problematic for numerous reasons, including that culpability assumes that people have chosen a course of action and thus should be made responsible for it. *Id.* at 163.

CONCLUSION

The writing is on the wall. One day soon, "[y]our phone — or in some years your glasses and, in a few more, your contact lenses — will tell you the name of that person at the party whose name you always forget . . . . Or it will tell the stalker in the bar the address where you live," or it will tell the police where you have been and where you are going.[441] FRT is rapidly moving society toward a world in which the Constitution's scope needs to be meaningfully reformulated, else it risks irrelevance when it comes to individuals' ability to hide from the prying eyes of government.[442] The third party doctrine and the longstanding judicial rejection of a reasonable expectation of privacy in matters made public have depleted the Fourth Amendment of vitality for purposes of establishing constitutional barriers to the government's use of FRT to profile and monitor individual citizens. Although the Court has expressly affirmed protections for anonymous speech under the First Amendment, that doctrine has not been extended to address the harms that flow from dragnet-style surveillance. Yet every member of the modern Court has at some point recognized that technology necessitates a rethinking of traditional constitutional boundaries.

This Article argued that existing First Amendment protections for anonymity should be brought to bear in assessing how Fourth Amendment doctrine can adapt to the challenges of modern surveillance methods. Today, the conglomerate of publicly available data is colossal and constantly expanding. Technology enables the government and private companies to identify patterns within such data which reveal new information that does not exist anywhere in isolation. As a consequence, information in the digital age is fundamentally distinct from information in the pre-digital age, in which the Court's Fourth Amendment doctrine evolved. This Article thus identified constitutionally derived guidelines for courts and lawmakers to consider in crafting judicial, legislative, and regulatory responses to the government's newfound capacity to create new information from storehouses of data gleaned from social media sites, public cameras, and increasingly sophisticated technologies like FRT. By giving these guidelines serious consideration, courts and lawmakers can tether foundational constitutional protections against over-surveillance with the development of the law—law that is otherwise broken and outdated.

---

441 Spencer, *supra* note 157 (quoting Professor Alessandro Acquisti).

442 *See* Gutterman, *supra* note 103, at 681 (construing *Katz* as "adher[ing] to the basic determination that fourth amendment protections must respond to technological developments").