2017

Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology

Mariko Hirose

CONNECTICUT
LAW REVIEW

VOLUME 49 SEPTEMBER 2017 NUMBER 5

Article

Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology

MARIKO HIROSE

Our society is steadily marching towards a world in which cameras equipped with facial recognition technology could be used to conduct constant and dragnet surveillance on people as they walk down the street. The law, as is usual in the field of privacy and emerging technologies, is lagging behind—no clear set of constitutional rules constrains law enforcement's use of this powerful technology, especially because the prevailing axiom has been that there is no right to privacy in public spaces. This Article challenges the axiom and argues that the dragnet, real-time uses of facial recognition technology violates reasonable expectations of privacy.

ARTICLE CONTENTS

I. INTRODUCTION 1593

II. THE CURRENT REALITY: INCHING TOWARDS THE DRAGNET, REAL-TIME USES OF FACIAL RECOGNITION 1596

A. EXPANDING LAW ENFORCEMENT USES OF FACIAL RECOGNITION TECHNOLOGY 1596

B. READY AVAILABILITY OF GOVERNMENT-OPERATED REFERENCE DATABASES 1598

III. THE USE OF FACIAL RECOGNITION TECHNOLOGY TO IDENTIFY PEOPLE ON THE STREETS IMPLICATES REASONABLE EXPECTATIONS OF PRIVACY 1600

A. PEOPLE MAINTAIN SUBJECTIVE EXPECTATIONS OF PRIVACY IN IDENTITY EVEN WHILE OUT IN PUBLIC 1601

B. THE SUBJECTIVE EXPECTATIONS OF PRIVACY IN IDENTITY WHILE OUT IN PUBLIC ARE REASONABLE. 1602

CONCLUSION 1620

Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology

MARIKO HIROSE*

[I]t is quite possible to find solitude in public. More importantly, it is also true that it is not necessary to be encased in a steel and glass container in order to do so. . . . [O]ne of the things strangers produce in their interactions with one another is privacy.[1]

I. INTRODUCTION

In October 2016, Governor Andrew M. Cuomo announced a "transformational plan to reimagine New York's bridges and tunnels for [the] 21st century."[2] Among over one-hundred pages of PowerPoint slides describing new flood protection, energy-efficient lighting, automatic tolling, and public art, were two that have the potential to transform, or even eviscerate, privacy as we know it.[3] These slides described the installation of "state-of-the-art facial recognition software and equipment" at every "crossing" into New York City and at airports and transit hubs like Penn Station, "ultimately becoming one system-wide plan."[4] It would open the door to the use of dragnet, real-time facial recognition—a world in which the government could, without any individualized suspicion, scan the faces of people in public and retrieve their identifying information.

Facial recognition has long triggered anxieties about a dystopian

---

* At the time of writing, the author was a Senior Staff Attorney at the New York Civil Liberties Union Foundation and an Adjunct Professor of Law at Fordham University School of Law and New York University School of Law. I am grateful to Aadhithi Padmanabhan, Rashida Richardson, and Ben Wizner for their insight and feedback and to Professor Marcus Aldredge of Iona College for taking the time to guide me through existing sociology research. All views expressed here are my own.

[1] LYN H. LOFLAND, THE PUBLIC REALM: EXPLORING THE CITY'S QUINTESSENTIAL SOCIAL TERRITORY 88 (1998).

[2] Press Release, MTA, Governor Cuomo Announces Transformational Plan to Reimagine New York's Bridges and Tunnels for 21st Century (Oct. 5, 2016), http://www.mta.info/news-governor-cuomo-bridges-and-tunnels-led-lights-open-road-tolling-automatic-tolling/2016/10/05 [perma.cc/f8HT-BAHB].

[3] N.Y. STATE, BUILDING TODAY FOR A BETTER TOMORROW: REIMAGINING NEW YORK'S CROSSINGS 25, 32, 54, 65 (2016), https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/MTACrossingsPresentation_2016.pdf.

[4] *Id.* at 44–45.

world. In the 2002 film *Minority Report*, Tom Cruise plays a hero in a world where there is no place to hide because facial recognition (and iris scanning technologies) allows the government to identify every person as they go about their daily lives. In such a world, there is no room for free speech, free thought, dissent, or human rights.

Despite the deep unease at the world of prevalent facial recognition, we continue to inch closer to that reality without an adequate discussion of the consequences. Aside from Governor Cuomo's proposal, a 2016 report from the Georgetown Law Center on Privacy & Technology identified five major American police departments at varying stages of interest in buying and using facial recognition technology that could be paired with real-time video surveillance.[5] The documentary film "Do Not Resist," also released in 2016, featured yet another type of real-time facial recognition already in use: in one scene, a Los Angeles police officer explains that she uses an automatic license plate scanner to identify wanted cars as she drives down the street and that she can now also use a scanner equipped with facial recognition technology in a similar manner.

This is only the beginning. We already live in a world with thousands of closed-circuit televisions (CCTVs) trained on our public movements and automatic license plate readers scanning the locations of our cars. New York City alone has a network of over 6,000 government and private cameras that are connected to one system—the Domain Awareness System—that also culls information from multiple government databases, automatic license plate readers, and gunshot spotters.[6] The rollout of police body cameras in localities across the country will bring tens of thousands more mobile cameras to the streets.[7] The future in which those cameras are equipped with facial recognition technology might not be in such a distant future.[8]

The law has not yet begun to grapple with the prospect of such a

---

[5] GEORGETOWN LAW CTR. ON PRIVACY & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 27 (2016) [hereinafter CPT REPORT], www.perpetuallineup.org.

[6] John J. Miller, Deputy Comm'r of Intelligence & Counterterrorism, Testimony Before the New York City Council Committees on Public Safety and Fire and Criminal Justice Services, New York City Police Department 4 (Nov. 12, 2014), http://www.nyc.gov/html/nypd/downloads/pdf/pr/terrorism_preparedness_testimony_11122014.pdf [perma.cc/55PP-HXBP]; NYC, DEVELOPING THE NYPD'S INFORMATION TECHNOLOGY 4–6, http://www.nyc.gov/html/nypd/html/home/POA/pdf/Technology.pdf [perma.cc/3RB3-GBR4].

[7] *See, e.g.*, *Justice Department Announces $20 Million in Funding to Support Body-Worn Camera Pilot Program*, DEP'T OF JUSTICE (May 1, 2015), https://www.justice.gov/opa/pr/justice-department-announces-20-million-funding-support-body-worn-camera-pilot-program [perma.cc/D9K6-35HK] (announcing $20 million in funding to support body-worn camera pilot program in local and tribal law enforcement organizations).

[8] *See, e.g.*, Ava Kofman, *Real-Time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, INTERCEPT (Mar. 22, 2017), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/ [perma.cc/8AJW-NJ5P].

future. Today, there is no comprehensive federal statute that governs the use of facial recognition technology in any of its forms, whether by private or public actors.[9] No court has yet decided the constitutional rules governing law-enforcement uses of facial recognition technology; indeed, higher courts are still in the process of deciding if and how the Fourth Amendment applies to surveillance technologies that have now been in use for decades, like cell phone location tracking, prolonged video surveillance, and license plate readers.[10] Moreover, this slowly emerging case law does not, at first glance, offer an obvious constitutional framework to apply to the use of facial recognition technology in public spaces, where the prevailing axiom has been that there is no right to privacy.[11]

This Article challenges the notion that there is no right to privacy in public and advances an argument for why dragnet, real-time use of facial recognition technology violates reasonable expectations of privacy protected under the Fourth Amendment. By dragnet, real-time uses, I mean the possibility of suspicionless and surreptitious law enforcement uses of cameras equipped with the technology (whether stationary or mobile) that can be used to scan people's faces as they go about their daily lives and to accurately match the faces with corresponding identifying information in an existing government database. The identifying information could be, for example, name and address combined with other information such as age, place of employment, immigration status, criminal record, arrest history, outstanding warrants and tickets, or perceived involvement in a gang.

This Article proceeds by describing the landscape of current law-enforcement uses of facial recognition technology and then by arguing that

---

[9] Certain existing laws, like the Privacy Act, may impose certain limitations on how the government can collect information in federal government databases that serve as reference databases for facial recognition technology. *See* Privacy Act of 1974, 5 U.S.C. § 552A(a)(4) (2012); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 2 (2016) [hereinafter GAO FBI REPORT], http://www.gao.gov/assets/680/677098.pdf [perma.cc/3YQU-PHP7].

[10] Although the Supreme Court held in *United States v. Jones* that the attachment of a GPS device implicates the Fourth Amendment, the Court did not reach the separate and "thorny" question of whether long-term location monitoring separately triggers Fourth Amendment concerns. United States v. Jones, 132 S. Ct. 945, 954 (2012). In 2016, petitions for certiorari to the Supreme Court were filed on cases that raise the constitutionality of warrantless cell phone location tracking, United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016) (en banc), *cert. filed*, No. 16-6308 (Sept. 26, 2016); United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016), *cert. filed*, No. 16-402 (Sept. 26, 2016), and the constitutionality of warrantless prolonged video surveillance, United States v. Houston, 813 F.3d 282, 285 (6th Cir. 2016), *cert. denied*, 2016 WL 4083077 (Dec. 5, 2016). Also in 2016, the New York Court of Appeals, the highest court in New York State, granted leave to hear a case challenging the suspicionless access to license plate databases. *New York v. Bushey*, 47 N.E.3d 96 (N.Y. 2016). As this Article is going to print, the Supreme Court granted certiorari in Carpenter v. United States.

[11] *See* Susan McCoy, Comment, *O'Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUTER & INFO. L.J. 471, 485 (2002) ("Facial-recognition is based on visual surveillance, which has long been held not to fall within the scope of the constitution . . . . [t]herefore, facial-recognition technology does not violate privacy rights").

reasonable expectations of privacy protect against its dragnet, real-time uses, drawing from prior legal scholarship, sociology research, and the past half-century of case law at the intersection of privacy and emerging technologies.[12] As the initial section makes clear, the prevalent and accurate use of facial recognition technology of the type that is the focus of this Article is still, thankfully, hypothetical due to technical limitations. The intent of the Article is to advance the discussion of how the existing Fourth Amendment framework protects against a future use of facial recognition before it is too late to step away from the brave new world of dragnet facial recognition.

II. THE CURRENT REALITY: INCHING TOWARDS THE DRAGNET, REAL-TIME USES OF FACIAL RECOGNITION

Facial recognition technology is one of many biometric technologies, or technologies that "identify individuals by measuring and analyzing their physiological or behavioral characteristics."[13] Facial recognition technology comprises a camera that captures an image of an unknown person and an algorithm that compares the "faceprint" (or "facial template") of the person in the image to those in a database of known people ("reference database").[14]

A. *Expanding Law Enforcement Uses of Facial Recognition Technology*

Certain law-enforcement uses of facial recognition technology are already prevalent at both federal and local levels.[15] The FBI now routinely uses facial recognition searches to identify individuals in the course of

---

[12] This Article builds on works of other scholars, including: Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 415 (2012); Douglas A. Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places*, 16 VA. J.L. & TECH 430, 462–63 (2011); Wayne A. Logan, *Policing Identity*, 92 B.U. L. REV. 1561, 1610–11 (2012); McCoy, *supra* note 11, at 492–93; Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L. REV. 213, 312–15 (2002).

[13] U.S. GOV'T ACCOUNTABILITY OFFICE, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 3 (2015), http://www.gao.gov/assets/680/671764.pdf [perma.cc/U9GG-J7NS]. Other biometrics that can be used for identification include fingerprints, handprints, irises, voice, and gait. *Id.*

[14] *Id.*; GAO FBI Report, *supra* note 9, at 5–6.

[15] For example, the New York State Department of Motor Vehicles uses facial recognition technology to identify individuals who attempt to obtain more than one identification document under different names. *See* N.Y. State, *Governor Cuomo Announces 13,000 Identity Fraud Cases Investigated by DMV Using Facial Recognition Technology*, OFFICE OF THE GOVERNOR (Mar. 5, 2013), http://www.governor.ny.gov/news/governor-cuomo-announces-13000-identity-fraud-cases-investigated-dmv-using-facial-recognition [perma.cc/8N88-7HKC]. The Center on Privacy & Technology report discusses a number of other ways in which facial recognition technology might be used. *See* CPT REPORT, *supra* note 5, at 10–12 (describing how law enforcement uses facial recognition technology to identify individuals who have been stopped or arrested, or are being investigated, as well as to identify individuals using real-time video surveillance).

criminal investigations: between August 2011 and December 2015, the FBI, as part of its own investigation or at the request of a state and local law enforcement agency, ran over 200,000 face recognition searches.[16] According to an estimate in the Center on Privacy & Technology report, more than one in four of all American state and local law enforcement agencies can "run face recognition searches of their own databases, run those searches on another agency's face recognition system, or have the option to access such a system."[17]

Most of these current, known law-enforcement uses of facial recognition technology do not involve the dragnet deployments of facial recognition technology that is the focus of this Article.[18] This is likely due to technical limitations. Even uses of facial recognition technology in controlled environments raise significant concerns about accuracy, especially for women, children, and African-Americans, for whom the existing facial recognition algorithms are known to be less accurate.[19] Dragnet, real-time facial recognition, in which the image of the individual is not taken in a controlled environment, is still more inaccurate and ineffective because of "computational limitations, video quality, and poor camera angles."[20]

Nevertheless, in addition to New York State, at least five local law enforcement agencies—the Los Angeles Police Department ("LAPD"), the West Virginia Intelligence Fusion Center, the Chicago Police Department, South Sound 911 in Washington, and Dallas Area Rapid Transit—already "either claim to use real-time video surveillance [with facial recognition software], have bought the necessary hardware and software, or have expressed written interest in buying it."[21] Of these departments, the LAPD has already installed at least sixteen surveillance cameras that are capable of recognizing faces at distances of up to six-hundred feet and identifying individuals who are on its hot lists of "wanted criminals or 'documented' gang members."[22]

Both the demand and the supply for more and better real-time facial recognition technology for law-enforcement use appear to be strong. Many private companies already sell real-time face recognition systems,

---

[16] *Id.* at 25.

[17] *Id.*

[18] *See id.* at 26–27 (discussing the risk levels associated with different forms of facial recognition technology usage in police agencies across the states). Such uses may also raise significant privacy and other concerns, especially depending on what reference database is used, but an analysis of these uses is beyond the limited scope of this Article.

[19] *See id.* at 53 ("The most prominent study, co-authored by an FBI expert, found that several leading algorithms performed worse on African Americans, women, and young adults than on Caucasians, men, and older people, respectively.").

[20] *Id.* at 29.

[21] *Id.* at 27.

[22] *Id.* at 23.

including NEC, Cognitec, 3M Cogent, Safran Identity & Security, Dynamic Imaging, and DataWorksPlus.[23] Vigilant Solutions, a company that sells subscriptions to its private database of automatic license plate reader data, also sells mobile facial recognition software for law-enforcement use.[24] Taser International, a company building police body cameras, plans to begin live-streaming body camera footage and using facial recognition.[25]

Although commercial uses of real-time facial recognition are outside the scope of this Article, private-sector supply and demand will likely push to improve this technology. One company already proposed a real-time facial recognition application that would have allowed the wearer of GoogleGlass to glance at a passerby and learn the person's name, occupation, and public Facebook profile information.[26] Although the deployment of that application was delayed following public outcry, other companies have moved forward with marketing real-time facial recognition software, including software that claims to allow churches to track parishioners or shops to identify suspected shoplifters.[27] Facebook's facial recognition algorithm has been reported to be 98% accurate, more accurate than the FBI's technology.[28] It seems inevitable that market forces, both private and public, will drive improvements in real-time facial recognition and its pervasiveness.

B. *Ready Availability of Government-Operated Reference Databases*

While it may take some years for real-time facial recognition technology to improve to the point of accuracy, once society reaches that reality law enforcement will already have access to a number of government-operated reference databases that can be used as a source of identification information. Today, the faces of over 117 million American adults are enrolled in a facial recognition reference database, and this

---

[23] *Id.* at 28–29.

[24] VIGILANT SOLUTIONS, https://vigilantsolutions.com/products/facesearch_facial_recognition [perma.cc/39BM-5WXY] (last visited Feb. 27, 2017).

[25] Matt Stroud, *Taser Plans to Livestream Police Body Camera Footage to the Cloud by 2017*, MOTHERBOARD (July 18, 2016), https://motherboard.vice.com/en_ca/read/taser-axon-police-body-camera-livestream [perma.cc/V7BH-6UEA].

[26] Natasha Singer, *Never Forgetting a Face*, N.Y. TIMES (May 17, 2014), http://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html [perma.cc/VTM2-YZUB].

[27] Robinson Meyer, *Who Owns Your Face?*, ATLANTIC (July 2, 2015), http://www.theatlantic.com/technology/archive/2015/07/how-good-facial-recognition-technology-government-regulation/397289/ [perma.cc/NW3B-G2EG].

[28] Naomi Lachance, *Facebook's Facial Recognition Software Is Different from the FBI's. Here's Why*, NPR (May 18, 2016, 9:30 AM), http://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why [perma.cc/N4H8-D6RN].

number is growing every day.[29]

One expansive reference database is the FBI's Next Generation Identification-Interstate Photo System (NGI-IPS), which contains 30 million photographs of an estimated 16.9 million individuals.[30] Nearly 20% of those photographs are "civil," in that they were submitted to the government in the course of licensing, employment, security clearances, military service, volunteer service, and immigration.[31] The remainder are "criminal," in that they were submitted by state and federal agencies as part of a lawful detention, arrest, or incarceration.[32]

But the NGI-IPS is not the only source of photographs and identification information. The Department of State maintains a collection of photographs from the Terrorist Screening Center database of "those known or reasonably suspected of being involved in terrorist activity," which can be searched using facial recognition technology.[33] Local law enforcement agencies maintain databases of suspected gang members, which often include booking photographs.[34] The use of these reference databases, which may include information about people who have not been convicted of any crimes but have come to the attention of law enforcement, raise significant concerns about accuracy, fairness, and racial bias, especially as people of color will be disproportionately and unfairly enrolled in such databases.[35]

Nor is the NGI-IPS the only source of "civil" photographs and identification, as a result of the expansion in government photo identification systems in the past half century. Drivers licensing was not required in all states until around 1960; now, over 87% of people over the

---

[29] CPT REPORT, *supra* note 5, at 2.

[30] GAO FBI Report, *supra* note 9, at 10 n.23.

[31] *See id.* at 11 ("The NGI-IPS database has two categories of photos: criminal identities (photos submitted as part of a lawful detention, an arrest, or incarceration), and civil identities . . . . Over 80 percent of the photos in NGI-IPS are criminal.").

[32] *Id.*

[33] *See id.* at 16 tbl.2 (noting that the Department of State uses the "Face Recognition on Demand" system to search photos from the Terrorist Screening Center database).

[34] *See* CAL. STATE AUDITOR, THE CALGANG CRIMINAL INTELLIGENCE SYSTEM 2015-130 11 (2016), https://www.auditor.ca.gov/pdfs/reports/2015-130.pdf [perma.cc/WAR6-TCH7] (describing the CalGang system, which, as of 2015, had the biographical information and booking photographs of 150,000 gang members or affiliate gang members).

[35] *See, e.g.*, Letter from Elaine M. Howle, CPA, State Auditor, to the Governor of Cal. & Legislative Leaders (Aug. 11, 2016), *in* CAL. STATE AUDITOR, *supra* note 34 (outlining audit findings of inaccuracies and inadequate oversight in the CalGang Criminal Intelligence System); CPT REPORT, *supra* note 5 (raising concerns about use of mug shots in reference databases, such as the inaccuracy of the technology, the disproportionate effects on African-Americans, and potential restriction of free speech); Jeremy Scahill & Ryan Devereaux, *Watch Commander: Barack Obama's Secret Terrorist-Tracking System, by the Numbers*, INTERCEPT (Aug. 5, 2014, 12:45 PM), https://theintercept.com/2014/08/05/watch-commander [perma.cc/V2KG-ZCKP] ("Nearly half of the people on the U.S. government's widely shared database of terrorist suspects are not connected to any known terrorist group . . . .").

age of sixteen in the United States have a driver's license,[36] and therefore have registered their face, name, current address, and other personal information with the Department of Motor Vehicles. Similarly, only seven million U.S. passports were in circulation in 1989; as of 2016, over 131 million U.S. passports were in circulation,[37] reflecting the number of people who have registered their face, name, and nationality with the Department of State.

Today, a government-issued photo ID is a necessary part of modern life, whether it is for driving, traveling, purchasing alcohol, entering government buildings, or verifying credit card purchases. While a more detailed legal analysis of the uses of facial recognition technology would require examining the specifics of the reference database used, what matters for this Article's thesis is that for years now people have been unwittingly enrolling in government databases that could be used in the future with facial recognition technology.

III. THE USE OF FACIAL RECOGNITION TECHNOLOGY TO IDENTIFY PEOPLE ON THE STREETS IMPLICATES REASONABLE EXPECTATIONS OF PRIVACY

The United States Supreme Court first rejected the axiom that privacy does not exist in public places in *United States v. Katz*.[38] In *Katz*, the FBI had, without a warrant, eavesdropped on a telephone conversation of the defendant, Charles Katz, who had made a phone call from a public telephone booth partly constructed of glass.[39] Because until then the Fourth Amendment was understood as protecting the right to privacy in property and prohibiting only trespass onto a constitutionally protected area such as a home, both parties focused their arguments on whether a public telephone booth was a constitutionally protected area.[40] The Court, however, rejected that framing of the issue, holding instead that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[41] The Court found that Katz's conversations were constitutionally protected under this proper framing of privacy interests because when he closed the door to the phone booth, he

---

[36] U.S. DEP'T OF TRANSP., FED. HIGHWAY ADMIN., *Our Nation's Highways: 2011*, https://www.fhwa.dot.gov/policyinformation/pubs/hf/pl11028/chapter4.cfm [perma.cc/3ZQT-X3FV] (last visited Feb. 25, 2017).

[37] U.S. DEP'T OF STATE, BUREAU OF CONSULAR AFFAIRS, *U.S. Passports & International Travel: Passport Statistics*, https://travel.state.gov/content/passports/en/passports/statistics.html [perma.cc/FJV6-2RXU] (last visited Feb. 25, 2017).

[38] 389 U.S. 347 (1967).

[39] *Id.* at 348, 352.

[40] *See id.* at 351 ("Because of the misleading way the issues have been formulated, the parties have attached great significance to the characterization of the telephone booth from which the petitioner placed his calls.").

[41] *Id.* at 351–52.

protected the contents of the conversation from "the uninvited ear," even if he did not protect the fact that he had made a phone call from "the intruding eye."[42]

Katz established that the Fourth Amendment protects privacy interests beyond those that are rooted in property rights, and, despite criticism of its "subjective and unpredictable" approach,[43] it remains the governing framework for evaluating such privacy interests.[44] Later cases analyzing *Katz* and drawing on Justice Harlan's concurrence in the case have explained that, under this approach, the Fourth Amendment protects legitimate or reasonable expectations of privacy where: (1) "the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy," and (2) "the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable."[45]

This *Katz* framework, properly viewed, strongly favors Fourth Amendment protection against the suspicionless and surreptitious use of facial recognition technology. Under *Katz*, the appropriate constitutional inquiry is whether people in contemporary American society have the reasonable expectation of privacy in identifying information about themselves even as they expose their faces to public view by leaving their homes and walking or driving down the street. The intuitively correct answer is yes, and so is the answer that *Katz*'s two-step inquiry yields.

A. *People Maintain Subjective Expectations of Privacy in Identity Even While Out in Public.*

Most people today exhibit subjective and actual expectations of privacy in their identities even while they are out in public. In walking down the street, we invite "the intruding eye" of strangers to glance at or even examine our faces as we pass by, but we do not invite them to also identify us by our names and addresses, much less occupation, immigration status, criminal history, and other personal information. People do not walk around in public announcing or displaying such identifying information, or giving out such information in response to inquiries. We teach children not to speak to strangers, and especially not to give out names and addresses to strangers. In many places, we expect to be able to take trips to the pharmacy to purchase sensitive items, or private trips to the doctor's office

---

[42] *Id.* at 352.

[43] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (acknowledging that the *Katz* test, which asks "whether the individual has an expectation of privacy that society is prepared to recognize as reasonable," has often been criticized as "circular, and hence subjective and unpredictable.").

[44] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 950 (2012) (explaining that *Katz* supplemented, but did not supplant, the traditional Fourth Amendment analysis rooted in the property-based approach to privacy).

[45] Smith v. Maryland, 442 U.S. 735, 740 (1979) (internal quotation marks omitted) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

or the therapist's office, or perhaps a quick trip to the grocery store in pajamas, with the minimal risk of being recognized and of being required to identify ourselves in public.[46]

The Supreme Court has affirmed this subjective expectation of privacy in First Amendment cases protecting the right to speak anonymously, most recently and explicitly in *Watchtower Bible and Tract Society of New York v. Village of Stratton*.[47] There, a village ordinance required individuals to obtain a license if they wanted to engage in door-to-door advocacy and distribution of handbills.[48] The court of appeals had rejected the First Amendment challenge to this ordinance, holding that it did not implicate constitutional interests in anonymous speech because a person already reveals their identity by appearing at someone's doorway to engage in advocacy.[49] The Supreme Court reversed, holding that the court of appeals' reasoning conflicted with First Amendment precedent holding that the fact that speakers "revealed their physical identities" did not foreclose the consideration of the speakers' "interest in maintaining their anonymity."[50] Even though speakers who are known to the residents of the village revealed their identities through face-to-face advocacy, strangers did not lose their privacy interests in their identities by revealing their faces in public.[51] In short, people do not lose their expectations of privacy in their identities by merely exposing their faces in public.

B. *The Subjective Expectations of Privacy in Identity While Out in Public Are Reasonable.*

This subjective expectation of privacy in identity is one that society is prepared to recognize as reasonable. Although the Supreme Court itself has acknowledged that there is "no talisman that determines in all cases those privacy expectations that society is prepared to accept as

---

[46] As discussed further below in *Hiibel v. Sixth Judicial Dist. Court of Nev.*, the Supreme Court held that a state law may require a person to identify themselves when a police stops the person as a result of reasonable suspicion that a person may be involved in criminal activity. Hiibel v. Sixth Judicial Dist. Court of Nev., 542 U.S. 177, 186–88 (2004). Short of that situation, however, a person cannot be compelled to identify themselves while in public. *See id.* at 184 (noting that when a stop is not based on "specific, objective facts establishing reasonable suspicion," the stop is impermissible) (citing Brown v. Texas, 443 U.S. 47, 52 (1979)).

[47] 536 U.S. 150 (2002).

[48] *See id.* at 154 ("[The ordinance] provides that any canvasser who intends to go on private property to promote a cause must obtain a 'Solicitation Permit' from the office of the mayor . . . .").

[49] *Id.* at 159, 166.

[50] *Id.* at 167.

[51] *See id.* ("The fact that circulators revealed their physical identities did not foreclose our consideration of the circulator's interest in maintaining their anonymity. In the Village, strangers to the resident certainly maintain their anonymity . . . ."); *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341 (1995) (noting that the First Amendment generally protects the freedom a speaker "to decide whether or not to disclose his or her true identity.").

reasonable,"[52] cases applying *Katz* have identified a few factors that either undermine or bolster the reasonableness of subjective expectations of privacy. On the one hand, an expectation of privacy is unreasonable if the information to be protected is exposed to the public or if it has already been shared with third parties. On the other hand, an expectation of privacy is reasonable if it comports with social norms and the intention of the Framers of the Constitution. I evaluate the expectation of privacy in identity under each of these factors to illustrate that this expectation is one that society has generally been prepared to recognize as reasonable.

1. *Identity Is Not Exposed to the Public Because of Practical Obscurity*

Under *Katz*, an expectation of privacy is not reasonable if the information at issue was "knowingly expose[d] to the public."[53] The Supreme Court has used this reasoning to deny privacy protections to people's faces and other physical characteristics that are exposed to the public, noting that a person cannot "reasonably expect that his face will be a mystery to the world."[54] The Court has also relied on this reasoning to deny privacy protections to visual surveillance from locations that are accessible to the public: thus, in *California v. Ciraolo*, the Court allowed the warrantless naked-eye inspection of the defendant's property from 1,000 feet in the air where private and commercial flights frequently travel,[55] and in *Florida v. Riley*, it allowed the same at 400 feet where helicopters travel.[56] The Court has also denied privacy protections to visual surveillance augmented by limited forms of technology: in *United States v. Knotts*, the Court permitted the warrantless use of a "beeper," a primitive tracking device, to supplement naked-eye surveillance in following a car on public roads for a short period of time.[57] Comparing the use of the beeper to the use of a searchlight, the Court held that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[58]

Unfortunately, this "public exposure" doctrine has been extended

---

[52] O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (O'Connor, J., plurality opinion); *see also* Kyllo v. United States, 533 U.S. 27, 34 (noting that reasonable privacy expectations need to be redefined as technologies continue to evolve).

[53] Katz v. United States, 389 U.S. 347, 347 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.").

[54] United States v. Dionisio, 410 U.S. 1, 14 (1973) (holding that a person does not have an expectation of privacy in his voice).

[55] 476 U.S. 207, 213 (1986).

[56] 488 U.S. 445, 450–51 (1989).

[57] *See* United States v. Knotts, 460 U.S. 276, 285 (1983) ("[T]here is no indication that the beeper was used in any way to reveal information . . . that would not have been visible to the naked eye . . . .").

[58] *Id.* at 282–83.

without adequate scrutiny to a type of technology that is similar in some respects to facial recognition technology—license plate look-ups and scanners. Using license plate look-ups and scanners, the police now have the capacity to retrieve identifying information about the car's owner in real-time, including name, address, date of birth, and outstanding warrants and tickets.[59] Every federal appellate court to confront the constitutionality of this practice has held that there is no constitutional protection against the suspicionless use of license plate look-ups because license plates are publicly displayed on a vehicle in plain view of law enforcement.[60]

But, as Judge Moore noted in dissenting from *United States v. Ellison*, the Sixth Circuit decision rejecting the right to privacy against the suspicionless use of license plate look-ups, fixating on the feasibility of visual surveillance in this context "misses the crux of the issue," not least because it "pays short shrift" to how the visual surveillance is used with information retrieved from a database.[61] In license plate look-ups as in facial recognition technology, the information that is private is not our faces or "the particular combination of letters and numerals that make up [the] license-plate number,"[62] but the aggregation of general information that a certain car or person was observed at a certain date, time, and place, with specific identifying information held in a government database.

---

[59] For example, in *State v. Donis,* a police officer conducted a random license plate check using a mobile data unit that retrieved the motorist's name, address, date of birth, and driver's license number, as well as other information. State v. Donis, 723 A.2d 35, 36 (N.J. 1998). In *People v. Bushey*, the defendant claimed that an officer similarly retrieved the motorist's name and address without any suspicion. *See* Brief of Appellant, People v. Bushey, No. 2016-00032 (N.Y. 2016). The court in *Bushey*, however, noted that the argument that the officer may have accessed private information was not preserved for review and that the officer had testified that the only relevant factor that he discovered before stopping the defendant as that his registration was suspended due to unpaid parking tickets. People v. Bushey, 2017 NY Slip Op 03560, n.2 (May 4, 2017).

[60] *See, e.g.*, United States v. Ellison, 462 F.3d 557, 561 (6th Cir. 2006) ("No argument can be made that a motorist seeks to keep the information on his license plate private. The very purpose of a license plate number . . . is to provide identifying information to law enforcement officials and others."); Olabisiomotosho v. City of Houston, 185 F.3d 521, 529 (5th Cir. 1999) (holding that "[a] motorist has no privacy interest in her license plate number"); United States v. Matthews, 615 F.2d 1279, 1285 (10th Cir. 1980) (holding that because a license plate is on the outside of a car, it is subject to seizure). One state court, the New Jersey Supreme Court, recognized concerns with suspicionless license plate look-ups that yield identifying information and ordered modifications to the system so that identifying information cannot be displayed unless there is reasonable suspicion. *See Donis*, 723 A.2d at 40 (N.J. 1998) ("[T]he data displays of the [mobile data terminal]s should be reprogrammed to provide for a two-step process. In the first step . . . . [t]he registered owner's personal information would not be displayed. If the original inquiry disclosed a basis for further police action, then the police officer would proceed to the second step, which would allow access to the 'personal information' of the registered owner . . . .").

[61] *Ellison*, 462 F.3d at 566–67 (Moore, J., dissenting). Judge Moore frames the appropriate question in analyzing license plate look-ups in the following manner: "[E]ven if there is no privacy interest in the license-plate number per se, can the police, without any measure of heightened suspicion or other constraint on their discretion, conduct a search using the license-plate number to access information about the vehicle and its operator that may not otherwise be public or accessible by the police without heightened suspicion?" *Id.* at 567.

[62] *Id.* at 566.

This aggregate, identifying portrait of a person that facial recognition technology enables is not exposed to the public simply because it is theoretically possible for a law enforcement officer to identify a person on a street through the combination of visual surveillance and a manual review of records. In *United States v. Maynard*, the Court of Appeals for the District of Columbia rejected this notion in a case involving location surveillance of a car using a GPS device.[63] In *Maynard*, the government had attached a GPS device to the defendant's car without a warrant and monitored its whereabouts for twenty-four hours a day for a month.[64] The court distinguished the case from *Knotts* because of the difference between the information that could be gleaned by the limited use of the beeper and the information that could be gleaned from GPS surveillance.[65] As the court explained:

> It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.[66]

The *Maynard* court concluded that aggregate information about a person's movement for a one-month period is not actually exposed to the public because "the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."[67] Nor is it constructively exposed to the public, even if each of the individual movements was exposed to the public, because it would be practically difficult for a person to observe each of those movements and because the aggregate whole revealed more private information about a person—including their habits, affiliations, and beliefs—than "any individual trip viewed in isolation."[68]

In coming to this conclusion, the court drew on case law from the Freedom of Information Act ("FOIA"). The court noted that in *United States Department of Justice v. Reporters' Committee for Freedom of Press*,[69] the Supreme Court found a privacy interest under FOIA in "rap sheets" that contain people's identifying information, including date of

---

[63] United States v. Maynard, 615 F.3d 544, 555–56 (D.C. Cir. 2010), *aff'd on other grounds sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[64] *Id.* at 555.

[65] *Id.* at 556.

[66] *Id.* at 560.

[67] *Id.*

[68] *Id.* at 561–62.

[69] *Id.* at 561 (citing U.S. Dep't of Justice v. Reporters' Comm. for Freedom of Press, 489 U.S. 749, 764–65 (1989)).

birth and physical characteristics, as well as a history of arrests, charges, convictions, and incarcerations in every jurisdiction around the country. The Court held that although each individual criminal record contained in the rap sheets was a public record that would be available to those who searched each courthouse file, county archives, and local police station in the country, the privacy of the aggregate summary of those records was protected by "practical obscurity"—that is, the practical difficulty of compiling the information.[70] Thus people maintained a privacy interest in the aggregate information "located in a single clearinghouse" even where individual records within that clearinghouse were public.[71]

The Supreme Court granted review in *Maynard*, which was re-named on appeal as *United States v. Jones*.[72] The majority opinion in *Jones* affirmed *Maynard* on the alternate theory that the warrantless attachment of the GPS implicated the Fourth Amendment's protection of property interests and did not validate or reject the *Maynard* court's theory of privacy.[73] But the five justices writing separately in *Jones* endorsed the conclusion in *Maynard* that location monitoring using GPS itself implicated the Fourth Amendment.[74] Justice Alito, concurring in the judgment and joined by Justices Ginsburg, Breyer, and Kagan, found reasonable the expectation of privacy in one-month of the defendant's movement history because of societal expectation that law enforcement agencies "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" for most offenses.[75] Justice Sotomayor, writing in concurrence, agreed with Justice Alito's conclusion and echoed the *Maynard* court's concerns about the comprehensive record of movement that can be gathered and revealed by GPS surveillance and the information it may reveal about the person's "familial, political, professional, religious, and sexual associations."[76] Five justices therefore effectively endorsed the view that the mere possibility of visual surveillance of individual vehicular trips from a public location does not undermine reasonable expectations of privacy.[77]

---

[70] *Reporters' Comm. for Freedom of Press*, 489 U.S. at 762–64, 780.

[71] *See id.* at 764–65 (finding the congressional intent "to protect the privacy of rap-sheet subjects, and a concomitant recognition of the power of compilations to affect personal privacy that outstrips the combined power of the bits of information contained within").

[72] 132 S. Ct. 945, 948–49 (2012).

[73] *Id.* at 953–54.

[74] *See id.* at 954–57 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"); *id.* at 964 (Alito, J., concurring) ("I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.").

[75] *Id.* at 964 (Alito, J., concurring).

[76] *Id.* at 954–57 (Sotomayor, J., concurring).

[77] Several state courts have also adopted similar approaches to privacy in GPS cases under their state constitutions. *See, e.g.*, New York v. Weaver, 909 N.E.2d 1195, 1199–1200 (N.Y. 2009)

The approach of *Maynard* and the five justices in *Jones* could be extended to argue that the aggregate information revealed as a result of the use of facial recognition technology on the streets is not publicly exposed, even if that information is about a person's presence in a location at one moment in time rather than their movement over a longer period. First, as explained above, the totality of information that could be revealed when facial recognition is used to identify an individual on the street is not information that is actually exposed to the public.[78] People do not walk around with signs announcing our identifying information. Indeed, the privacy interest implicated by the identification of people walking on the street is far greater than the interest implicated by license plate look-ups, because people do not, and are not required to, walk around with signs displaying identification information that they registered to the government.[79]

Second, that information is not constructively exposed to the public because of "practical obscurity." Without facial recognition technology and a clearinghouse of information, it would require a "super recognizer," a person with extraordinary skill at recognizing faces in crowds, to identify an individual and to retrieve information about that person as they are walking by. Research suggests that such "super recognizers" exist and that at least one police department is taking advantage of their abilities in pursuing investigations,[80] but the limited number of people with such skills necessarily ensures that their skills are only used for investigations that need them. Facial recognition lifts the resource constraints that have served as a practical protection for privacy, just as the advent of GPS surveillance lifted the resource constraints that ensured that intrusive, prolonged location surveillance was employed only against the most serious offenders that warranted the time and attention of multiple police

(recognizing that GPS monitoring "yields . . . a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits"); Washington v. Jackson, 76 P.3d 217, 223 (Wash. 2003) (en banc) ("In this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and foibles.").

[78] *See supra* Section III.A (providing examples of information not typically visually available to the public such as names, addresses, occupation, immigration status, and criminal history).

[79] In cases involving license plate look-ups, courts have noted that "[t]he very purpose of a license plate number, like that of a Vehicle Identification Number, is to provide identifying information to law enforcement officials and others." *See, e.g.*, United States v. Ellison, 462 F.3d 557, 561 (6th Cir. 2006); *see also* People v. Bushey, 2017 NY Slip Op 03560 (rejecting any expectation of privacy against license plate look-ups because one of the important objectives of motor vehicle registration is to "facilitate the identification of the owner" (internal quotation marks omitted)).

[80] *See* Patrick Radden Keefe, *The Detectives Who Never Forget a Face*, NEW YORKER (Aug. 22, 2016), http://www.newyorker.com/magazine/2016/08/22/londons-super-recognizer-police-force [perma.cc/95YY-Z8CE] ("In Room 901 of New Scotland Yard, the police had assembled half a dozen officers who shared an unusual talent: they all had a preternatural ability to recognize human faces.").

officers over days and weeks.[81]

Finally, the information revealed by the use of facial recognition clearly implicates privacy interests that are different from, and more than, the sum of its parts. A database of a person's photograph, name, address, and other personal information on its own holds a wealth of private information about a person. But that information is far more valuable when it is combined with an image depicting the person's presence at a protest, the person's entry into a gay bar, an abortion clinic, or a mosque, or the person's interactions with another identifiable person.[82] That these discrete pieces of information may be accessible to law enforcement does not mean that the combination of those pieces of information is exposed to the public.

2. *Identity in Public Is Not Subject to the Third-Party Doctrine Because it Is Not Voluntarily Shared with Government Entities.*

Under *Katz*'s progeny, the Supreme Court has held that information loses its privacy protection where it is voluntarily disclosed to a third-party. This doctrine, known as the "third-party doctrine," developed in the 1970s—but, as with the public exposure doctrine just discussed, should not apply to the use of facial recognition technology.

In *United States v. Miller*, decided in 1976, the Court held that there was no Fourth Amendment right to privacy in bank records because these records "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[83] The Court found that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[84] This was so even if the information was shared to a third party "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[85]

In following *Miller* in 1979, the Court further held in *Smith v. Maryland* that there was no Fourth Amendment right to privacy in telephone dialing records of a home line.[86] The Court found that any subjective expectations of privacy in numbers dialed were not reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[87] In short, because a person voluntarily chooses to share phone dialing information with the telephone

---

[81] *See* Jones, 132 S. Ct. at 964 (Alito, J., concurring) (finding that GPS devices have made long-term monitoring "relatively easy and cheap").

[82] *See* New York v. Weaver, 909 N.E.2d 1195, 1199–1200 (N.Y. 2009).

[83] 425 U.S. 435, 442 (1976).

[84] *Id.* at 443.

[85] *Id.*

[86] 442 U.S. 735, 744 (1979).

[87] *Id.* at 743–44.

company in making a call, the person has "assumed the risk that the company would reveal to the police the numbers he dialed."[88]

But the third-party doctrine does not apply to the use of facial recognition technology on the streets for the same reason that the public exposure doctrine does not apply. In *Miller* and *Smith*, the government sought to obtain only the limited business records that were in the possession of the third-party businesses pursuant to ordinary business practices. With facial recognition, however, law enforcement not only seeks access to identification records already existing in some government database, but seeks to dip into that database to generate new information that links a person's location with the identifying information. People have not handed over to any third-party the aggregate information generated by the use of facial recognition technology— the information of where they are in a given moment in time combined with identifying information.[89]

Moreover, that identifying information exists in a government database does not mean that any government agency has the right to access it for law-enforcement purposes. *Ferguson v. City of Charleston* establishes one of the limitations to such access.[90] In that case, a public hospital worked with law enforcement to set forth procedures by which the hospital staff would test pregnant patients suspected of drug use and refer any positive tests to law enforcement for arrest and prosecution.[91] Even though medical records are prototypical of records that are always shared with third parties, namely doctors, the Court did not apply the third-party doctrine in that case.[92] Instead, it held that the patients maintained a "reasonable expectation of privacy" that the results of their diagnostic tests "will not be shared with nonmedical personnel without her consent."[93] As in *Ferguson*, when people share their identifying information with one government entity for a limited purpose, they do not voluntarily consent to the use of that information in combination with facial recognition for all future law enforcement purposes.

This leads to an important point about voluntariness. *Miller* and *Smith* held that the expectations of privacy in those cases were unreasonable because the defendants voluntarily agreed to share their information with third-parties when they elected to use a service offered by a private

---

[88] *Id.* at 744.

[89] In certain instances this type of information will be in the hands of the third party. If a person chooses to email a friend using Gmail that she is in a certain location, the government may try to access that information through Gmail. If a person is carrying a cell phone, the government may try to access location information through the cell phone provider. But these are separate questions from whether the third-party doctrine applies to the government attempting to access this information through the use of facial recognition technology.

[90] 532 U.S. 67, 85–86 (2001).

[91] *Id.* at 70–73.

[92] *See id.* at 78.

[93] *Id.*

business.[94] The same cannot be said for those whose pictures and personal information are recorded by the government in the course of criminal proceedings and enrolled in a government reference database—to the contrary, they are disclosing this information under coercion. More broadly, the same also cannot be said for a person's decision to forfeit their private identifying information to the government in order to apply for a benefit that only the government can offer and that is critical to modern life, such as government-issued photo identification. In a similar vein, some courts have rejected the notion that people voluntarily share their location information with their cell phone providers by their decision to use their cell phone because a cell phone is a modern necessity.[95]

Finally, *Miller* and *Smith* were decided in such a different technological reality that it may no longer make sense to apply the third-party doctrine to today's world, as Justice Sotomayor posited in her *Jones* concurrence.[96] The information that could be accumulated and analyzed about a person in the 1970s, whether through bank records or through telephone dialing records, was limited by technology and storage costs. By comparison, today the speed at which society produces data has accelerated—according to one announcement, 90% of the data in the world has been generated in two years.[97] The Supreme Court already recognized in the 1970s that the "accumulation of vast amounts of personal

---

[94] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[The] petitioner had to convey [the dialed] number to the telephone company . . . if he wished to complete his call."); United States v. Miller, 425 U.S. 435, 442 (1976) ("All documents obtained . . . contain only information voluntarily conveyed to the banks . . . .").

[95] *See, e.g.*, *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) ("The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone must be rejected"); Tracey v. Florida, 152 So. 3d 504, 523 (Fla. 2014) (rejecting the application of *Miller* and *Smith* to location records held by a cell phone provider because "[r]equiring a cell phone user to turn off the phone just to assure privacy from government intrusion that can reveal a detailed and intimate picture of the user's life places an unreasonable burden on the user to forego necessary use of his cell phone, a device now considered essential by much of the populace"). *But see, e.g.*, United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (en banc) (holding that a defendant had no reasonable expectation of privacy in his cellphone carrier's business records showing the cell tower locations of his phone calls); United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc) (holding that a defendants had no reasonable expectations of privacy in historical cell-site location information), *cert. filed*, No. 16-6308 (Sept. 26, 2016); United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016) ("Carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls. And carriers keep records of these data to find weak spots in their network and to determine whether roaming charges apply, among other purposes. Thus, the cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves. The government's collection of business records containing these data therefore is not a search"), *cert. filed*, No. 16-402 (Sept. 26, 2016).

[96] *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (expressing doubt over the third-party doctrine given that, in the digital age, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

[97] *What is Big Data?*, IBM, https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html [perma.cc/SJ4R-47U7] (last visited Feb. 27, 2017).

information in computerized data banks or other massive government files" raises significant privacy concerns, especially when not accompanied by adequate protections against unwarranted disclosure.[98] The massive databases that are possible today, and that are readily accessible by facial recognition technology, render the third-party doctrine of *Miller* and *Smith* anachronistic to the privacy threats that exist today.

3. *Social Norms Validate the Privacy in Identity.*

The previous two sections discussed factors that undermine reasonable expectations of privacy, but what about factors that bolster reasonableness of expectations in privacy? The Supreme Court has stated that expectations of privacy are reasonable where they are "established by general social norms."[99]

On the one hand, general social norms inform us to expect some level of intrusive behavior from others in society while we are in public spaces. In *California v. Greenwood*, the Court held that general social norms undermined the reasonableness of the expectation of privacy in the contents of garbage bags left on the streets because "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[100]

On the other hand, society frowns on intrusive behavior in public that crosses a certain threshold. Thus, in *Bond v. United States*, the Supreme Court held that a law enforcement agent violated reasonable expectations of privacy by squeezing a bag that a traveler had stored in the overhead storage area of a bus.[101] The Court explained that while a bus passenger expects that his bag may be handled, "[h]e does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner."[102] *Bond* drew a distinction between the minimally-intrusive surveillance that can be expected in public, such as the aerial surveillance in *Ciraolo* and *Riley*, and the tactile intrusion that occurred in the case.[103]

---

[98] Whalen v. Roe, 429 U.S. 589, 605–06 (1977) (citation omitted) (rejecting challenge to a state prescription database, but recognizing concern regarding unwarranted disclosures of personal information resulting from government collection of information); *see also id*. at 606–07 (Brennan, J., concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.").

[99] California v. Greenwood, 486 U.S. 35, 51 n.3 (1988) (quoting Robbins v. California, 453 U.S. 420, 428 (1981)); *see also* Rakas v. Illinois, 439 U.S. 128, 143–44 n.12 (1978) (stating that reasonableness of expectations of privacy can be rooted in "understandings that are recognized or permitted by society").

[100] *Greenwood*, 486 U.S. at 40 (footnotes omitted).

[101] Bond v. United States, 529 U.S. 334, 338–39 (2000).

[102] *Id.* at 338–39.

[103] *See id.* at 337 ("Physically invasive inspection is simply more intrusive than purely visual

Lower courts have recognized that, even without the tactile intrusion of *Bond*, intensive visual surveillance in public can cross the line of socially acceptable norms. Some courts have therefore held that prolonged video surveillance of the exterior of a person's home, even if taken from a lawfully accessible location, violates reasonable expectations of privacy.[104] Some state courts have held that aerial surveillance violates reasonable expectations where the airplane hovers above a person's property and causes an intrusion into a sphere of privacy that exceeds the "brief flyover" visual surveillance of *Ciraolo* and *Riley*.[105]

Facial recognition surveillance, like these forms of more intrusive surveillance, crosses the boundaries of socially acceptable behavior in public. Although the Supreme Court has not clearly delineated the sources of such norms, one place to search for norms is in sociology literature. In the 1970s, sociologist Erving Goffman coined the term "civil inattention" to describe the social rules that people follow in navigating pedestrian traffic in the streets.[106] While walking on the streets, we constantly scan our surroundings, including others who are sharing the streets with us. But this scan is limited to a "simple body check," a brief glance to ensure that the two people are not on a collision path.[107] Staring at a person's facial features—the non-technological equivalent to facial recognition—is socially unacceptable and "may be construed as an encroachment or threat of some kind."[108] The natural defense of those caught staring at passersby in public is to "enact a scan that gives the appearance of happening to fall upon the victim the moment he happens to look at the scanner."[109]

Goffman further explained that this level of information control over one's identity is necessary to navigate the various spaces in people's lives—spaces where we are likely to be known personally and spaces where we "can expect to remain anonymous, eventful to no one."[110] And while Goffman focused his analysis on those who he believed would suffer

---

inspection."); *see also supra* Section III. B.1 (discussing *Riley* and *Ciraolo*).

[104] *See, e.g.*, United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987) (holding that prolonged video surveillance of the curtilage of the defendants' home from a utility pole implicated the Fourth Amendment); Shafer v. City of Boulder, 896 F. Supp. 2d 915, 931–32 (D. Nev. 2012) (recognizing a reasonable expectation of privacy against constant video surveillance of defendant's backyard for fifty-six days). *But see* United States v. Houston, 813 F.3d 282, 287–88 (6th Cir. 2016) (holding that a ten-week video surveillance of the defendant's farm from a camera located on top of a public utility pole on the road did not implicate the Fourth Amendment).

[105] New Mexico v. Davis, 360 P.3d 1161, 1172 (N.M. 2015); *see also, e.g.*, Vermont v. Bryant, 950 A.2d 467, 480–81 (Vt. 2008) (holding the same under the Vermont State Constitution).

[106] ERVING GOFFMAN, RELATIONS IN PUBLIC: MICROSTUDIES OF THE PUBLIC ORDER 209 (1971).

[107] *Id.* at 12.

[108] *Id.* at 132.

[109] *Id.* at 127; *see also id*. at 59 (those who seek to stare at others in a fixed location must relegate themselves to the "few places available that are sufficiently far removed from other persons present"). Other scholars have written on the need for privacy in public spaces. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 555–56 (2006) (discussing work of Irwin Altman).

[110] ERVING GOFFMAN, STIGMA: NOTES ON THE MANAGEMENT OF SPOILED IDENTITY 83 (1963).

stigma if certain personal information about themselves were revealed, he recognized that every person has some situation in which they will need to manage the disclosure of their identities.[111]

Lyn H. Lofland, writing about urban public space in the 1990s, also noted that civil inattention "makes possible copresence without commingling, awareness without engrossment, courtesy without conversation"—and that it is "the sine qua non of city life."[112] She concluded that "when humans in the public realm appear to ignore one another, they do so *not* out of psychological distress but out of a ritual regard, and their response is *not* the asocial one of 'shut down' but the fully social one of politeness."[113] Society depends on the norm of maintaining some respectful distance from fellow humans as each person goes around their daily lives.

Goffman coined the term "civil inattention" decades ago, but recent polls confirm that privacy in identity in public places continues to be a valued social norm. According to a 2015 poll conducted by Pew Research, over 60% of the American public believe that being able to travel in public without always being identified is an important societal value.[114] In further support of this belief, 93% of those surveyed believed it important to maintain control of who can get information about them.[115] In a separate Pew Research survey, 95% of those surveyed responded that their social security number—the ultimate identifier—was sensitive information, more sensitive than health records or the content of phone conversation.[116]

There is widespread recognition, evident in popular culture as well as the media coverage on this topic, that the use of facial recognition to identify individuals in public will violate the prevailing norms of society.[117] The Fourth Amendment should protect these norms of privacy

---

[111] *See id.* at 127 ("The most fortunate of normal is likely to have his half-hidden failing, and for every little failing there is a social occasion when it will loom large, creating a shameful gap between virtual and actual social identity.").

[112] LOFLAND, *supra* note 1, at 30.

[113] *Id.*

[114] PEW RESEARCH CTR., AMERICANS HOLD STRONG VIEWS ABOUT PRIVACY IN EVERYDAY LIFE (May 19, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/pi_15-05-20_privacysecurityattd00/ [perma.cc/8TBB-C9ZC].

[115] *Id.*

[116] MARY MADDEN, PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [perma.cc/GRS3-3T53].

[117] *See, e.g.*, Andrew Liszewski, *This Creepy Facial Recognition System Knows How Often You Visit a Store*, GIZMODO (Nov. 12, 2012, 12:40 PM), http://gizmodo.com/5959723/this-creepy-facial-recognition-system-knows-how-often-you-visit-a-store [https://perma.cc/7QY4-H6VDF]; Richard Newton, *You Are Being Watched: Face Recognition Deemed 'Creepy' By UK Shoppers*, GUARDIAN (July 27, 2015, 2:15 PM), https://www.theguardian.com/small-business-network/2015/jul/27/you-are-being-watched-face-recognition-creepy-uk-shoppers [perma.cc/V2CD-QKM7]; Singer, *supra* note 26; Keith Wagstaff, *Washington Frets Over 'Minority Report'-Style Facial Recognition Technology*, NBC NEWS (Dec. 4, 2013, 6:26 PM), http://www.nbcnews.com/technology/washington-frets-over-minority-report-style-facial-recognition-technology-2D11692143 [https://perma.cc/7HAU-PEDU].

that exist today.

4. *The Intent of the Framers of the Constitution to Prohibit Indiscriminate Searches, Prevent Arbitrary and Discriminate Intrusions, and Support Democratic Principles Validates the Privacy in Identity.*

Courts also look to the "intention of the framers of the Fourth Amendment" in determining the reasonableness of expectations of privacy.[118] In the case of facial recognition, there is of course no explicit evidence of intent—it is safe to say that the Founding Fathers could not have imagined the world of electronic databases that exist today, much less the technology that can match that data with a face in real-time. But facial recognition impinges on several concepts that were critical to the Framers in crafting the Constitution, including the prohibition on general searches, the prevention of arbitrary and indiscriminate intrusion on privacy, and the preservation of a democracy. As some judges have already suggested, these factors should be used as guide posts in determining the reasonableness of expectations of privacy in the modern world.[119]

i. The potential for indiscriminate searches.

In crafting the Constitution, and in particular the Fourth Amendment, the Framers sought to prevent "indiscriminate searches and seizures" like those that were conducted under the authority of general warrants.[120] Courts have therefore noted the need to be vigilant against technologies that enable "dragnet-type law enforcement practices"[121] and "programs of mass surveillance."[122] In *Knotts*, the Court rejected the defendant's

---

[118] O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

[119] *See, e.g.*, United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring) (rejecting *Maynard*'s approach to reasonable expectations of privacy but suggesting that he would determine the constitutionality of GPS surveillance by exploring whether there are colorable arguments that "the use of GPS technology to engage in long-term tracking is analogous to general warrants that the Fourth Amendment was designed to curtail . . . the technology's potential to be used arbitrarily or because it may alter the relationship between citizen and government in a way that is inimical to democratic society"), *rev'd*, United States v. Jones, 132 S. Ct. 945 (2012); *see also Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (describing the "attributes of GPS monitoring" that she would take into account when considering the existence of reasonable expectations of privacy, including the potential of the technology to "evade[] the ordinary checks that constrain abusive law enforcement practices" and to "alter the relationship between citizen and government in a way that is inimical to democratic society" (internal quotation marks and citations omitted)).

[120] Payton v. New York, 445 U.S. 573, 583 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment."); *see* also Boyd v. United States, 116 U.S. 616, 625–27 (1886) (describing the history of general warrants).

[121] United States v. Knotts, 460 U.S. 276, 283–84 (1983).

[122] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) (rejecting constitutional challenge to warrantless GPS surveillance in the case but noting that "[s]hould government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search").

suggestion that beeper surveillance would permit twenty-four hour surveillance of any citizen in the country without judicial knowledge or supervision, but stated that "if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[123]

That time may arrive with advanced uses of facial recognition technology. When facial recognition is used with real-time video surveillance, mass surveillance is the reality, not only a mere possibility. Other uses of facial recognition technology, like a mobile scanner that can be pointed at any person the street, also facilitate the indiscriminate uses of the technology because they, by their surreptitious nature, "evade[] the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility."[124] Given this potential for mass surveillance, the use of facial recognition technologies should be subject to some Fourth Amendment regulation.

ii. The potential for arbitrary and discriminatory intrusion by the police.

At the core of the Fourth Amendment is "[t]he security of one's privacy against arbitrary intrusion by the police."[125] Indeed, the Supreme Court has prohibited police officers from stopping and demanding identification from a person walking on the street,[126] or for that matter from a person driving down the road,[127] without suspicion because "the risk of arbitrary and abusive police practices exceeds tolerable limits."[128] It is only when officers have reasonable suspicion for stopping a person in the first place that the law enforcement interest in demanding to know the person's name exceeds the privacy interest in one's identity.[129]

Facial recognition technology subverts these long-standing Fourth Amendment protections by allowing the police to discover the identities of anyone on the streets, and without any constitutional limitations, the technology will likely result in widespread abuse and misuse. A recent

---

[123] *Knotts*, 460 U.S. at 283–84.

[124] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (internal quotation marks and citations omitted).

[125] Wolf v. Colorado, 338 U.S. 25, 27–28 (1949) (internal quotation marks omitted) (holding that the Fourth Amendment is "implicit in the concept of ordered liberty" and enforceable against the States under the Due Process Clause).

[126] Brown v. Texas, 443 U.S. 47, 52–53 (1979).

[127] Delaware v. Prouse, 440 U.S. 648, 663 (1979).

[128] *Brown*, 443 U.S. at 52 (citing *Prouse*, 440 U.S. at 661).

[129] Hiibel v. Sixth Judicial Dist. Court of Nev., 542 U.S. 177, 187–88 (2004) ("The reasonableness of a seizure under the Fourth Amendment is determined 'by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests'. . . . A state law requiring a suspect to disclose his name in the course of a valid Terry stop is consistent with Fourth Amendment prohibitions against unreasonable searches and seizures." (internal citation omitted)).

Associated Press report uncovered evidence of nationwide abuse and misuse of confidential law enforcement databases to learn private information about romantic partners, journalists, and others for reasons unrelated to law enforcement.[130] An audit of law enforcement access to a license records database in Minnesota in 2012 found that more than half of the users audited had queried people with the same last name or disproportionately searched for people of one sex.[131] In Florida, more than 400 incidents of misuse of the state's Driver and Vehicle Information Database was reported in an 18-month period starting in 2014.[132]

This pattern of abuse and misuse is also likely to disproportionately impact communities of color. Even when well-established case law has required reasonable suspicion for law enforcement to stop individuals, people of color have been stopped disproportionately and discriminatorily targeted by the police.[133] In a world where the police are free to direct surveillance technologies to anyone without any suspicion, the scrutiny is likely to fall on communities of color. As Justice Sotomayor noted recently, "it is no secret that people of color are disproportionate victims of this type of [suspicionless] scrutiny [by the police]."[134]

The impact on these communities will be both psychological and physical. As Judge Moore noted in dissent in *Ellison*, the case regarding the suspicionless use of license plate look-ups, there is real, cognizable harm in "[t]he psychological invasion that results from knowing that one's personal information is subject to search by the police, for no reason . . . ."[135] This is the psychological privacy harm that *Katz* protects even when there is no intrusion on property interests.[136]

But the harm of facial recognition technology will not stop at the

---

[130] Sadie Gurman & Eric Tucker, *AP: Across US, Police Officers Abuse Confidential Databases*, Associated Press (Sept. 28, 2016, 12:28 AM), http://bigstory.ap.org/article/699236946e3140659fff8a2362e16f43/ap-across-us-police-officers-abuse-confidential-databases [perma.cc/4U8L-FJV6].

[131] OFFICE OF THE LEGISLATIVE AUDITOR, STATE OF MINN., EVALUATION REPORT: LAW ENFORCEMENT'S USE OF STATE DATABASES 25–26 (2013), http://www.auditor.leg.state.mn.us/ped/pedrep/ledatabase.pdf [https://perma.cc/HS7W-PYU9]; Eric Roper, *Audit Finds Common Misuse of Minnesota Driver Data*, STAR TRIB. (Sept. 13, 2013, 5:56 AM), http://www.startribune.com/feb-21-audit-finds-common-misuse-of-minnesota-driver-data/192090631/?c=y&page=all&prepage=1#continue [https://perma.cc/SQ79-HDL5].

[132] Howard Altman, *Misuse of Florida's Driver Database Is Often Personal*, TAMPA BAY ONLINE (Aug. 27, 2016), http://www.tbo.com/news/crime/misuse-of-floridas-driver-database-is-often-personal-20160827/ [https://perma.cc/4PUX-SRL3].

[133] *See e.g.*, Floyd v. City of New York, 959 F. Supp. 2d 540, 562 (S.D.N.Y. 2013) ("[T]he City adopted a policy of indirect racial profiling by targeting racially defined groups for stops based on local crime suspect data. This has resulted in the disproportionate and discriminatory stopping of blacks and Hispanics in violation of the Equal Protection Clause. Both statistical and anecdotal evidence showed that minorities are indeed treated differently than whites.").

[134] Utah v. Strieff, 136 S. Ct. 2056, 2070 (2016) (Sotomayor, J., dissenting).

[135] United States v. Ellison, 462 F.3d 557, 568 (6th Cir. 2006) (Moore, dissenting).

[136] *See* Katz v. United States, 389 U.S. 347, 359 (1967) ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

psychological if the technology is used to manufacture a reason to stop and investigate a person—that is, if it is used not only to retrieve identifying information, but also information about a person's outstanding warrants, tickets, or other information that will give police officers "reasonable suspicion" or "probable cause" to stop a person. Unfortunately, in *Utah v. Strieff*, the Supreme Court recently approved an arrest and a search incident to arrest that occurred after an initial illegitimate stop of the person turned up an outstanding warrant.[137]

Strieff, however, should be limited to its facts and should not apply to endorse law enforcement's suspicionless use of facial recognition technology. The Supreme Court's decision in *Strieff* was premised on its belief that the suspicionless warrant check that occurred in the case was "an isolated instance of negligence" and therefore did not raise the specter of dragnet searches.[138] As explained above, the government's decision to allow suspicionless use of facial recognition technology is a decision to allow dragnet searches of people's identities.[139] Such use of facial recognition would create precisely the world that Justice Sotomayor fears in her dissent in *Strieff*—a world where officers can "warrant-check random joggers, dog walkers, and lemonade vendors just to ensure they pose no threat to anyone else."[140]

Such a world would significantly alter the current balance of interactions between people and law enforcement. As Justice Sotomayor noted:

> Outstanding warrants are surprisingly common. When a person with a traffic ticket misses a fine payment or court appearance, a court will issue a warrant. When a person on probation drinks alcohol or breaks curfew, a court will issue a warrant. The States and Federal Government maintain databases with over 7.8 million outstanding warrants, the vast majority of which appear to be for minor offenses. Even these sources may not track the "staggering" numbers of warrants, " 'drawers and drawers' " full, that many cities issue for traffic violations and ordinance infractions. The county in this case has had a "backlog" of such warrants. The Department of Justice recently reported that in the town of Ferguson, Missouri, with a population of 21,000, 16,000

---

[137] *See Strieff*, 136 S. Ct. at 2064 ("We hold that the evidence . . . seized as part of [the officer's] search incident to arrest is admissible because his discovery of the arrest warrant attenuated the connection between the unlawful stop and the evidence seized . . . .").

[138] *Id.* at 2063.

[139] *See supra* Section III.B.4(i).

[140] Utah v. Strieff, 136 S. Ct. 2056, 2067 (2016) (internal citations omitted) (Sotomayor, J., dissenting).

people had outstanding warrants against them.[141]

With the number of outstanding warrants and tickets, which themselves are known to disproportionately and unfairly impact communities of color,[142] the suspicionless use of facial recognition to identify person's outstanding warrants and tickets will result in an exponential increase in the number of people who are subjected to "[t]he indignity of the [law enforcement] stop" as they go about their daily lives.[143] These stops have serious consequences beyond the momentary detention, including the potential of an intrusive search and an escalating encounter that could result in a violent end.[144] The Fourth Amendment needs to be interpreted to intervene against such a reality.

iii. The potential to undermine fundamental values of democracy

Finally, the Constitution exists "to safeguard fundamental values."[145] Facial recognition has the potential to undermine those fundamental values, including many that are enshrined in the Bill of Rights apart from the Fourth Amendment. Used to monitor those engaged in free speech and advocacy, it may infringe on the First Amendment right to anonymous

---

[141] *Id.* at 2068 (Sotomayor, J., dissenting) (internal citations omitted).

[142] For example, although marijuana is used at comparable rates by whites and blacks, according to data from 2010, "a black person was 3.73 times more likely to be arrested for marijuana possession than a white person." ACLU, THE WAR ON MARIJUANA IN BLACK AND WHITE 9 (2013). In the report on the Ferguson Police Department, the U.S. Department of Justice noted the cumulative impact of disparate impact:

> African Americans are more likely to be searched but less likely to have contraband found on them; more likely to receive a citation following a stop and more likely to receive multiple citations at once; more likely to be arrested; more likely to have force used against them; more likely to have their case last longer and require more encounters with the municipal court; more likely to have an arrest warrant issued against them by the municipal court; and more likely to be arrested solely on the basis of an outstanding warrant.

CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE FERGUSON POLICE DEPARTMENT 71 (2015).

[143] *Strieff*, 136 S. Ct. at 2070 (Sotomayor, J., dissenting).

[144] *See id.* at 2070 ("The indignity of the stop is not limited to an officer telling you that you look like a criminal. The officer may next ask for your 'consent' to inspect your bag or purse without telling you that you can decline. Regardless of your answer, he may order you to stand 'helpless, perhaps facing a wall with [your] hands raised.' If the officer thinks you might be dangerous, he may then 'frisk' you for weapons. . . . 'A thorough search [may] be made of [your] arms and armpits, waistline and back, the groin and area about the testicles, and entire surface of the legs down to the feet.' . . . For generations, black and brown parents have given their children 'the talk'—instructing them never to run down the street; always keep your hands where they can be seen; do not even think of talking back to a stranger—all out of fear of how an officer with a gun will react to them." (internal citations omitted)).

[145] United States v. Chadwick, 433 U.S. 1, 9 (1977) ("What we do know is that the Framers were men who focused on the wrongs of that day but who intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth."), *abrogated by* California v. Acevedo, 500 U.S. 565, 579 (1991).

speech.[146] Used to monitor travel, it may infringe on the freedom of movement.[147] Used to collect and disclose private information about a person, such as their medical conditions, it may infringe on the right to informational privacy.[148]

More broadly, constant and dragnet facial recognition brings the society closer to a system of national identification, in which the government has the power and authority to identify and locate an individual at any moment. As Professor Richard Sobel has argued in the context of the proposal to create national identity cards, such systems "fundamentally contradict the bases of the American system of governance."[149] Identification systems "have a long history of being used for social control and discrimination,"[150] including in slavery,[151] in the Holocaust,[152] and in Japanese-American internment.[153] Such systems contradict American principles and freedoms and "demean[] political and personal identity by transforming personhood from an intrinsic quality inhering in individuals . . . [into] an attribute of bureaucratic and computerized systems."[154] As Professor Sobel concludes: "The spontaneity of human existence, the right to be let alone, the seclusion of privacy, and the pursuit of happiness need to be revered and preserved."[155]

In her *Strieff* dissent, Justice Sotomayor sounded in similar sentiment in opposing a search that resulted from an unlawful stop and warrant check:

> By legitimizing the conduct that produces this double consciousness, this case tells everyone, white and black, guilty and innocent, that an officer can verify your legal status at any time. . . . It implies that you are not a citizen of a democracy but the subject of a carceral state, just waiting to

---

[146] *See* Slobogin, *supra* note 12, at 246–51 ("There is little doubt that public camera surveillance can infringe First Amendment values"); *see also supra* Section III.A.

[147] *See* Slobogin, *supra* note 12, at 262–63 (discussing case law and concluding that the case law "suggests that public surveillance, even when targeting actions not protected by the First Amendment, can infringe interests in locomotion and statis to a legally cognizable degree").

[148] The Supreme Court has referenced, but not clarified, the concept of right to information privacy against the disclosure of personal information. *See* Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 138 (2011) (assuming, but not deciding, whether a constitutional right to informational privacy applies). However, circuit courts have recognized such a right in various instances. *See e.g.*, Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994) (recognizing the right to privacy in confidentiality of one's HIV status).

[149] Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J. L. & TECH. 319, 320 (2002).

[150] *Id.* at 343.

[151] *Id.*

[152] *Id.* at 344.

[153] *Id.* at 348–49.

[154] *Id*. at 320.

[155] *Id.* at 382.

be cataloged.[156]

Dragnet use of facial recognition technology opens the door precisely to the cataloguing of individuals as they go about their daily lives. It is fundamentally inconsistent with the values of democracy.

CONCLUSION

In this Article, I have attempted to advance an argument against the suspicionless use of facial recognition technology using the *Katz* framework. There are, of course, limitations to the Article. There is more work to be done to refine the concept of "identity" used throughout the Article; more sociology and psychology research that could be consulted to bolster the argument for societal norms against facial recognition; more law to analyze depending on the precise purpose and use of the facial recognition technology, including the reference database used; and more complications to untangle in what the reasonable expectations of privacy mean for judicial supervision of the use of the technology and for suppression motions in the criminal context. There are fundamental questions about the limitations of the *Katz* framework itself, including how it would apply to the extent dragnet uses of facial recognition technology become common-place, commercially or otherwise.[157]

In discussions about privacy and emerging technologies, the central question is whether the Fourth Amendment will continue to protect existing societal norms and democratic principles, or if the pace of technological changes will eviscerate them. I hope that this Article adds to the ongoing conversations about the implications of facial recognition technology for our democracy and privacy, particularly if they are used in a dragnet, suspicionless, real-time manner.

---

[156] Utah v. Strieff, 136 S. Ct. 2056, 2070–71 (2016).

[157] In *Kyllo v. United States*, the Court recognized the right to privacy against the use of heat-detection technology, but specifically noted that the government was using a device "that is not in general public use." Kyllo v. United States, 533 U.S. 27, 40 (2001). This has left open the question of how the right to privacy would continue to protect people if and once certain intrusive surveillance technologies become available for common use.