VIRGINIA JOURNAL OF LAW & TECHNOLOGY

FALL 2011 UNIVERSITY OF VIRGINIA VOL. 16, NO. 03

Face-Recognition Surveillance: *A Moment of Truth for Fourth Amendment Rights in Public Places*

DOUGLAS A. FRETTY†

ABSTRACT

Americans are increasingly monitored with face-recognition technology (FRT), a surveillance tool that allows the state to identify a pedestrian based on a pre-existing database of facial photographs. This Article argues that FRT embodies the fundamental Fourth Amendment dilemmas raised by contemporary digital surveillance and will serve as a harbinger for the Amendment's future. FRT cases will test whether people retain a reasonable expectation of privacy in their identities when they move in public, and whether the aggregation of information about a person's movements amounts to an unreasonable search. Further, the suspicionless identification of pedestrians will test whether a seizure can occur without the government's halting a person's locomotion, and whether the probable-cause standard is offended by FRT software's substantial false-positive rate. The compiling of photo databases should also push courts to decide whether the third-party disclosure doctrine is tenable in an age when Americans routinely disclose personal information to ISP providers.

† Douglas Fretty is an associate at Irell & Manella, LLP, in Los Angeles, California. He received his J.D. in 2011 from UCLA School of Law and his B.A. in 2005 from Brown University.

TABLE OF CONTENTS

I. INTRODUCTION

Since the 2001 Super Bowl, when Tampa Bay installed face-recognizing cameras in its stadium to catch criminals attending the big game, Americans have been increasingly monitored with face-recognition technology (FRT). Though the technique remains crude, face-based surveillance is already used in airports and on city streets to detect fugitives, teenage runaways, criminal suspects, or anyone who was ever arrested. As it spreads, FRT will be an unusually fraught topic for courts to address, because it straddles so many fault lines currently lying beneath our Fourth Amendment jurisprudence. These include whether: (1) people enjoy a reasonable expectation of anonymity in public, (2) a seizure can occur without halting a person's movement, (3) long-term aggregation of data about individuals can constitute a search, and (4) the probable-cause standard tolerates generalized surveillance with a high rate of false positives. These fault lines are not minor questions but fundamental challenges of the digital-surveillance movement. While most courts to address these issues have erred toward *diminished* Fourth Amendment protection, this Article cites an emerging minority that would reclaim basic privacy rights currently threatened by electronic monitoring in public.

Part II of this Article describes FRT's present and future uses by government. Municipalities are the most visible experimenters in faced-based surveillance, equipping their police officers with face-scanning devices or installing FRT-enhanced cameras in public thoroughfares. The U.S. government's FRT investment is less conspicuous, but reports from the Defense Advanced Research Project Agency (DARPA) and the Disruptive Technology Office indicate the agencies' hopes of using FRT to track high-priority suspects. Part III considers in depth whether identifications of civilians in public can constitute unreasonable searches or seizures. While two commentators have argued that the Fourth Amendment offers no protection to people identified on the street,[1] this Article asserts that the Amendment's terrain is much more complex and that FRT will probe the fissures already visible in search-and-seizure law. The results of facial-surveillance suits, then, will presage the Amendment's robustness in the coming decades. Part IV explores possible statutory and constitutional limits to the government's building of photo databases (or "photobases"). The two laws intended to curb the federal government's compilation of citizens' private information—the Privacy Act of 1976 and the Electronic Stored Communications Act—will fail to prevent most acts of photo-basing by U.S. agencies. However, the Fourth Amendment has the potential to protect commercially-held photos, such as those posted on Facebook, from government scrutiny under a recent string of opinions challenging the traditional "third-party disclosure" doctrine. Finally, Part V asks whether an FRT algorithm with a substantial failure rate can establish probable cause for the search or detention of an identified person. Though certain evidence-gathering tools with high false-positive rates are tolerated under *Illinois v. Gates*, society's interest in preventing unnecessary police harassment should demand an exacting level of accuracy from FRT surveillance.

II. PRESENT AND FUTURE USES OF FRT

Since at least the early 1990s, researchers in universities, private firms, and the U.S. military have been developing algorithms for recognizing humans based on their facial features. As the authors of the Department of Defense's face-recognition experiment known as FERET explain, such algorithms typically perform two consecutive tasks: normalization and identification.[2] Normalization consists of centering the subject's eyes along a pre-established grid, removing pixels of hair or inanimate obstructions, and locating key facial features.[3] The identification phase then quantifies those key features, reduces them to a small file,[4] and compares the file to a database of pre-identified facial

[1] *See* Nguyen, *infra* note 4; Breinholt, *infra* note 43.

[2] P. J. Phillips et al., *The FERET Evaluation Methodology For Face Recognition Algorithms*, 22 IEEE TRANSACTIONS ON PATTERN ANALYSIS & MACHINE INTELLIGENCE 1090, 1091 (2000). FERET was a joint venture of the U.S. National Institute of Standards and Technology, the U.S. Department of Defense Counterdrug Technology Development Program, performed in part at the U.S. Army Research Laboratory. *Id.* at 1103. The stated purpose of the program was "to assess the state-of-the-art and the feasibility of automatic face recognition." *Id.* at 1090.

[3] *Id.* at 1094.

[4] Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2, at nn.30–35 (2002) (summarizing an FRT process used by the private company FaceIt).

images.[5] The algorithm determines whether the unknown subject matches a databased photo,[6] and the confidence level of a match.[7]

The reliability of contemporary face-recognition programs is a subject of some mystery. Following the attacks of September 11, 2001, Congress directed the National Institute of Standards and Technology (NIST) to evaluate all commercially available FRT programs.[8] NIST's last testing, performed in 2002, concluded that the best-performing system identified faces with 90% accuracy when indoors but with only 50% accuracy outdoors.[9] When Boston's Logan International Airport introduced a trial FRT system in 2003, the estimated failure rate was 38.6%,[10] and airports that followed Logan's lead similarly struggled with system failures.[11] Researchers recently estimated that the accuracy of FRT algorithms in identifying anonymous pedestrians averaged only 60%.[12] These and other results have led antiterrorism specialist Stephen Graham to caution that FRT "is only effective when people stand in line in decent lighting conditions," such as at a border crossing or security screening.[13] Still, using close-ups of unknown faces dramatically increases an algorithm's competence, and surveillance clips of several seconds are increasingly likely to produce accurate matches.[14] Technology companies and research scientists frequently announce FRT innovations that promise to accelerate efficiency while minimizing error.[15]

---

[5] Dozens of facial features can be reduced to quantifiable values. As Nguyen explains, the company FaceIt quantifies eighty distinct facial areas, though the company maintains that its algorithms can identify faces using only fourteen areas. *Id.* *See also* Tilen Mlakar et al., *Face Image Registration for Improving Face Recognition Rate*, STAR, Jan. 2008, at 43 (algorithm identifies individuals based on eye contour); Xiaona Xu et al., *Multimodal Recognition Fusing Ear and Profile Face Based on KPCA*, ISSCAA 2008: THE 2ND INT'L SYMP. ON SYS. AND CONTROL IN AERONAUTICS & ASTRONAUTICS 130 (2009) ("Ear recognition has been proved to be a promising subject in biometrics authentication.").

[6] In conducting the FERET program, Phillips et al. tested algorithms' ability to resist making false positives. Phillips et al., *supra* note 2, at 1091.

[7] In the FERET experiments, confidence levels were expressed as "similarity scores." *Id.* at 1093.

[8] This instruction is a provision of the USA PATRIOT Act of 2001, 8 U.S.C. § 1379 (2001).

[9] P. JONATHAN PHILLIPS ET AL., FACE RECOGNITION VENDOR TEST 2002: OVERVIEW AND SUMMARY 8 (Mar. 2003), *available at* http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf. A later incarnation of FERET, the Face Recognition Vendor Test (FRVT) is a joint venture of NIST, the Defense Advanced Research Projects Agency (DARPA), and the Department of Defense Counterdrug Technology Development Program. The best-performing systems experienced a 1% false-positive rate. *Id.* at 5.

[10] HARRY WECHSLER, RELIABLE FACE RECOGNITION METHODS: SYSTEM DESIGN, IMPLEMENTATION AND EVALUATION 4 (2007).

[11] WILLIAM D. EGGERS, GOVERNMENT 2.0: USING TECHNOLOGY TO IMPROVE EDUCATION, CUT RED TAPE, REDUCE GRIDLOCK, AND ENHANCE DEMOCRACY 199 (2005).

[12] Angshul Majumdar & Panos Nasiopoulos, *Frontal Face Recognition from Video*, ADVANCES IN VISUAL COMPUTING: 4TH ANNUAL SYMP., ISVC 2008, PART II, LNCS 279 (2008).

[13] Stephen Graham, *Specters of Terror, in* CITY OF COLLISION: JERUSALEM AND THE PRINCIPLES OF CONFLICT URBANISM 157 (Philipp Misselwitz, ed., 2006). *See also* Charles Piller et al., *Criminal Faces in the Crowd Still Elude Hidden ID Cameras*, L.A. TIMES, Feb. 2, 2001, at 1.

[14] Majumdar & Nasiopoulos, *supra* note 12, at 304–05 (describing experiment that compared two algorithms and noted that as video clip duration increased from one second to eight seconds, the algorithms' accuracy elevated from 83% and 65%, respectively, to 96% and 99%, respectively).

[15] *See, e.g.*, Yi-Min Wen & Zhi-Gang Fan, *Discriminative Feature Selection for Fast Face Recognition*, J. NAT'L U. DEF. TECH., May–June 2009, at 87–91; J. Sheeba Rani et al., *Robust Face Recognition Using Wavelet Transform and Autoassociative Neural Network*, 1 INT'L J. BIOMETRICS 231

A. How the Technology is Used Today

Despite the technical uncertainty, numerous public and private entities are incorporating FRT into their operations, as part of the larger biometric technology boom.[16] Companies engaged in extensive e-commerce, for example, are investing in systems that consummate online transactions only when the identity of the parties has been verified via webcam.[17] In addition, many commercial and government buildings with restricted access identify authorized persons by some biometric characteristic,[18] with facial scanning expected to become more prevalent.[19] The most popularly-used application of FRT is an online program called Polar Rose, purchased by Apple in September, 2010 for a rumored $29 million.[20] Polar Rose uses a person's tagged photographs to derive a three-dimensional image of the subject's face, and then searches the internet for all photographs of that person.[21] Thus, a search reveals photographs published without the subject's authorization.[22] A natural exploitation of Polar Rose is to enhance background checks on job applicants,[23] a prospect that should alarm young people, whose photographs are the most likely to be published on the internet in large, indiscriminate batches.[24]

Of course, government adoption of FRT marches apace, as it is "heralded by military and security technology companies as a means to track known suspects."[25]

(2008); N. C. Nguyen & J. Peraire, *An Interpolation Method for the Reconstruction and Recognition of Face Images*, STAR, Jan. 2008.

[16] *See* Nguyen, *supra* note 4 ("The use of biometric technology is predicted to be one of the fastest-growing industry fields today.").

[17] *See* S. Liu & M. Silverman, *A Practical Guide to Biometric Security Technology*, IT PROF., Jan. 2001, at 27–32 (evaluating the range of biometric identification technology available for e-commerce); Anil Jain et al., *Biometric Identification*, COMM. OF THE ACM, Feb. 2000 ("E-commerce and e-banking are two of the most important application areas" of biometric identification).

[18] Trevor T. Adler, *Privacy Implications of Commercial Office Building Security Technology in the Post-9/11 Era*, 8 COLUM. SCI. & TECH. L. REV. 91, 102 (2007).

[19]Christopher S. Milligan, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDIS. L.J. 295, 307 (1999).

[20] *See* Mike Butcher, *Apple buys Polar Rose for a rumored 29 million*, TECHCRUNCH EUR. (Sept. 20, 2010), http://eu.techcrunch.com/2010/09/20/apple-buys-polar-rose-for-a-rumoured-22-million/ (updated to correct earlier price tag of $22 million).

[21] Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1872 (2007).

[22] *Id.* at 1874.

[23] *Id.* at 1887.

[24] *See* Andrew L. Mendelson & Zizi Papacharissi, *Look At Us: Collective Narcissism in College Student Facebook Photo Galleries*, in A NETWORKED SELF: IDENTITY, COMMUNITY, AND CULTURE ON SOCIAL NETWORK SITES 251, 258–64 (Zizi Papacharissi, ed., 2010), *available at* http://temple.academia.edu/AndrewMendelson/Papers/228605/Look_At_Us_Collective_Narcissism_in_College_Student_Facebook_Photo_Galleries. Many employers currently analyze job applicants' Facebook profiles to glean additional information, even though the social networking site's policies "suggest that an organization may face legal challenges if it considers an applicant's Facebook page as part of the selection process." William P. Smith & Deborah L. Kidder, *You've Been Tagged! (Then again, maybe not): Employers and Facebook*, 53 BUS. HORIZONS 491, 491 (2010).

[25] Graham, *supra* note 13, at 157.

Police famously scanned the crowds at the 2001 Tampa Bay Super Bowl with FRT,[26] identifying nineteen criminal suspects but making no arrests.[27] Salt Lake City spent fourteen months equipping the security for its 2002 Winter Olympics with face-scanning surveillance, though the Organizing Committee made an eleventh-hour decision not to employ the technology.[28] High-profile events aside, cities are embracing FRT to monitor their citizens on a daily, more mundane basis. Many municipalities, including Los Angeles and New York City, have equipped police officers with facial scanners that determine whether a suspect has a criminal record,[29] while others install the technology on stationary street cameras.[30] Several states are building databases of driver's license photos, anticipating that the database could support future FRT systems,[31] with airports as a focus for many FRT projects.[32]

The federal government's activeness in this arena is hard to measure, but the Department of Defense has historically shown great enthusiasm for "human identification at a distance," or "HumanID."[33] Shortly after the USA PATRIOT Act passed in 2001,[34] DARPA established a data-mining and pattern-recognition program "to provide tools to better detect, classify, and identify potential foreign terrorists."[35] Called TIA (originally "Total Information Awareness" but redubbed "Terrorism Information Awareness" to

---

[26] Rob Turner, *The Way We Live Now: Salient Facts: Facial-Recognition Technology; Faceprinting*, N.Y. TIMES, Aug. 12, 2001, at 18 (recounting Tampa's use of FRT at the 2001 Super Bowl).

[27] Vince Horiuchi, *Fingers, Faces Will Be Scanned, Oly Security May Raise Legal Issues; Games Security Adds Face Scans and Fingerprints*, SALT LAKE CITY TRIB., Nov. 30, 2001, at D1; Garry Barker, *Big brother watches from the outer; EXCLUSIVE: The net closes on known criminals as surveillance goes on a controversial step further*, SUNDAY AGE, THE (Melbourne), Feb. 11, 2001, at 4.

[28] Accounts differ over whether the decision was based on FRT's technological feasibility or commercial disputes among the event's security contractors. Barnaby J. Feder, *Maker of Crowd Scanner Is on Defensive Again*, N.Y. TIMES, Feb. 18, 2002, at C3.

[29] Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321, 1341 (2008); Kameel Stanley, *A Picture Is Worth a Thousand Names*, ST. PETERSBURG TIMES, July 21, 2009 (reporting on officers' use of hand-held facial scanners in Pinellas, Florida); Edward Lewine, *Face-Scan Systems' Use Debated*, ST. PETERSBURG TIMES, Dec. 8, 2001, at 3B (reporting on officers' use of FRT in Ybor City, Florida); Michelle Morgan Bolton, *Now, an App for Fighting Crime; Brockton PD to Use iPhone Face Scans*, BOSTON GLOBE, Jul. 15, 2010, at 6 (describing police use of FRT in Brockton, Massachusetts); *Early Show: New York City Police to Scan Crowds with Surveillance System that Uses Facial Recognition to Pick Out Known Criminals* (CNBC News Transcripts May 24, 2002).

[30] Darryl McAllister, *Law Enforcement Turns to Face-Recognition Technology*, INFORMATION TODAY, May 2007, at 50 (describing installation of FRT on the streets of Virginia Beach, Virginia). New York City is in the process of equipping lower Manhattan with three thousand surveillance cameras, reserving the option to interface the cameras with FRT. Murphy, *supra* note 29, at 1341–42.

[31] *Id.* at 1342 (citing Adam Liptak, *Driver's License Emerges as Crime-Fighting Tool, but Privacy Advocates Worry*, N.Y. TIMES, Feb. 17, 2007, at A10).

[32] Karen Alexander, *Airport to Get Facial Recognition Technology; Oakland: The Equipment Will Be Used to Identify Suspects Who Have Been Arrested. Privacy Advocates Raise Concerns*, L.A. TIMES, Oct. 29, 2001, at 1.

[33] DEF. ADVANCED RESEARCH PROJECTS AGENCY, REPORT TO CONGRESS REGARDING THE TERRORISM INFORMATION AWARENESS PROGRAM 10–11 (2003), available at http://www.epic.org/privacy/profiling/tia/may03_report.pdf [hereinafter TIA REPORT].

[34] Ron Wyden et al., *Spies, Secrets, and Security: The New Law of Intelligence: Oversight of Intelligence: Law and Policy Efforts to Balance Security, Privacy and Civil Liberties in Post-9/11 America*, 17 STAN. L. & POL'Y REV 331, 340 (2006).

[35] TIA REPORT, *supra* note 33, at 3.

avoid an overtly Orwellian moniker),[36] the program included a HumanID component, intended to "identify humans using a combination of biometric modes at distances up to 500 feet."[37] In a 2003 report to Congress, DARPA revealed that its then-existing HumanID technology could detect the presence of human faces at 20 to 150 feet "and then zoom[] in to recognize the detected face."[38] Members of Congress, disturbed by TIA's potential invasiveness, defunded the program in the fall of 2003.[39] Nevertheless, TIA appears not to have vanished but merely moved to the Disruptive Technology Office,[40] a department under the auspices of the Director of National Intelligence.[41] DARPA's 2003 report, then, likely describes not simply FRT research conducted in the past but ongoing activity in the U.S. intelligence community.[42]

B. The Foreseeable Evolution of State-Run FRT

In the relatively near term, we can imagine arenas into which government use of FRT will expand. The potential usefulness of FRT in combating crime will encourage municipalities to proliferate video surveillance in public spaces,[43] as is already conspicuously occurring in London, which monitors its citizenry with over 200,000 cameras.[44] In addition, agencies may seek increased access to private surveillance systems[45] through court orders, administrative subpoenas,[46] or simple volunteerism: in Washington, D.C., many owners of commercial property shared their security camera feeds with the city police after the attacks of September 11, 2001 (hereinafter 9/11 attacks).[47] Because an FRT system is only as useful as its photo database, agencies may seek to expand their databases of pre-identified faces, a task that could be accomplished in any of three ways: (1) combining publicly-held facial photos, such as from passports,

---

[36] Wyden et al., *supra* note 34, at 342.

[37] TIA REPORT, *supra* note 33, at A-18.

[38] *Id.* As the Report also boasts, "In 2 years, the program has reduced error rate on recognition from frontal indoor images by 50 percent. The development of three-dimensional morphable models has greatly increased the capability to recognize nonfrontal faces." *Id.* at A-18-19.

[39] Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 450-51 (2008). The publicity generated by the introduction of TIA also highlighted the potential for mass government spying on civilians. *See* John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2003, at A1.

[40] Cate, *supra* note 39, at 451.

[41] In 2007 the Disruptive Technology Office was incorporated into a new program in the office of the Director of National Intelligence called the Intelligence Advanced Research Projects Agency (IARPA), modeled after the Department of Defense's own DARPA. *Intel agencies get their own 'ARPA,'* AEROSPACE DAILY & DEF. REP., Nov. 19, 2007, at 2 .

[42] FRT was recently used to confirm the death of Osama Bin Laden. Mark Mazzetti et al., *Behind the Hunt for Bid Laden*, N.Y. TIMES, May 3, 2011, at A1.

[43] Jeff Breinholt, the former Deputy Chief of the DOJ Criminal Division, Counterterrorism Section, posits that as biometric identification becomes more efficient and less invasive, the justification for blanketing urban areas with surveillance receptors becomes ever more compelling. Jeff Breinholt, *Review Essay: Getting Real About Privacy: Eccentric Expectations in the Post-9/11 World*, 2005 U. ILL. J.L. TECH. & POL'Y 273 (2005).

[44] Bob Barr, *Symposium on Electronic Privacy in the Information Age: Post-9/11 Electronic Surveillance Severely Undermining Freedom*, 41 VAL. U.L. REV. 1383, 1401 (2007).

[45] *See generally*, Adler, *supra* note 18.

[46] *See id.* at 106.

[47] Barr, *supra* note 44, at 1405.

driver's licenses, and arrest mug shots;[48] (2) collecting commercially-held photos, such as from social networking websites;[49] and (3) requiring photo-taking at newly created checkpoints, such as airports or government offices.[50]

The goals of government-run FRT could be narrowly concerned with detecting suspected terrorists, as DARPA suggested in its report to Congress.[51] However, the federal government's current data-aggregating activities foretell FRT's much broader utility, as the National Crime Information Center (NCIC) hosts files on a dizzying array of persons the government has an interest in tracking, such as "missing persons, unidentified persons, criminal suspects wanted by law enforcement, sex offenders, federal prisoners, persons on parole or probation, suspected terrorists, gangs, persons enrolled in the U.S. Marshal [sic] Service's Witness Security Program, victims of identity theft, [and] foreign fugitives . . . ."[52]

Beyond tracking individuals already on a government watch-list, FRT's data-mining capabilities are intended to recommend *new* suspects.[53] For example, a police department could theoretically cross-reference surveillance footage between a high-drug-volume housing project[54] and a nearby airport, revealing which project residents most frequent the airport,[55] and thus producing evidence of possible drug trafficking. In the

[48] Phillips et al., *supra* note 2, at 1090; Murphy, *supra* note 29, at 1342.

[49] Facebook reports that it receives approximately 1,000 requests per month from government agencies for disclosure of user data. Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359, 394 (2010). This figure does not include National Security Letters, administrative subpoenas that forbid the recipient from disclosing that the request was made. *Id.*

[50] This technique was advocated in the TIA Report, which predicts, "Biometric signatures will be acquired from various collection sensors including video, infrared and multispectral sensors." TIA REPORT, *supra* note 33, at 10–11. Jeff Breinholt also advocates this method of collecting what he describes as "gait identification" information, consisting of a brief video recording of how a person walks, which recording can later be used to identify the person at a distance. Breinholt, *supra* note 43, at 273–75.

[51] TIA REPORT, *supra* note 33, at 3.

[52] Cate, *supra* note 39, at 443–44 (noting that as of 2003, "the NCIC contained 71 million state criminal history files," and that as of 2006 the FBI's Investigative Data Warehouse contained "more than 659 million records, which come from 50 FBI and outside government agency sources.")

[53] In a process called "link analysis," police already use data-mining techniques to "graphically display[] connections between groups, individuals, and organizations." JESUS MENA, INVESTIGATIVE DATA MINING FOR SECURITY AND CRIMINAL DETECTION 82–84 (2003). For an example of link analysis that exploits video footage of political protests, see Kirsten Christiansen, *The Conquest of Space: New York City's New Frontier of Social Control, in* SURVEILLANCE AND GOVERNANCE: CRIME CONTROL AND BEYOND 70 (Mathieu Deflem, ed. 2008).

[54] Police already assert a more visible presence in high-drug-volume neighborhoods and install denser networks of surveillance cameras in housing projects associated with drug trafficking. *See* Andrew Guthrie Ferguson & Damien Bernache, *The "High-Crime Area" Question: Requiring Verifiable and Quantifiable Evidence for Fourth Amendment Reasonable Suspicion Analysis*, 57 AM. U.L. REV. 1587, nn.120, 275, 292 (2008) (citing cases where "high-drug" neighborhood justified elevated levels of searches and seizures); Milligan, *supra* note 19, at 323 (describing installation of surveillance cameras in high-crime housing projects in Boston, Massachusetts to curb crime).

[55] For decades, police have staked out airports and followed "drug courier profile" guidelines intended to detect which passengers are most likely to be carrying contraband. *See generally*, Stephen E. Hall, *A Balancing Approach to the Constitutionality of Drug Courier Profiles*, 1993 U. ILL. L. REV. 1007 (1993). Factors inputted into the drug courier profile include the city of origin, the city of destination, the method

national-security context, the FBI is suspected of gathering embarrassing personal information about American Muslims to pressure them into informing on their fellow mosque-attendees.[56] Such a tactic can be aided by FRT, which could cross-reference the exteriors of mosques with other, compromising locations such as homosexual establishments or bankruptcy offices.

C. The Impact on Privacy Interests

Parts III-V of this article evaluate how FRT comports with U.S. privacy *law*, but first it is worth noting what traditional privacy *interests* are threatened by an expansive state use of FRT. Two distinct privacy interests at stake are dignity and control of access.[57] The theory that privacy has inherent worth because it preserves human dignity was first offered in 1964 by Edward J. Bloustein.[58] Bloustein observed that when a person's actions or personality are subject to a threshold level of scrutiny, the person's concept of himself as autonomous and independent dissolves.[59] Under this theory, the question is whether Americans' being facially identified in public, and subject to scrutiny by government officials, would erode their self-image as autonomous personalities. A second school of commentators argues that one's ability to control the access that others have to him/her is a fundamental human interest, and that privacy rights are the guardian of that interest.[60] This theory holds that people need a certain dominion over when and whether they will interact with others, and that secrecy, anonymity, and solitude are the tools with which we exercise that dominion.[61] FRT, then, threatens privacy if it removes peoples' expectation of secrecy, anonymity, and solitude while moving in the public sphere.

Whether we can exercise our privacy interests also impacts our enjoyment of liberty. Michael Foucault famously argued in *Discipline and Punish* that a system capable of locating a person, identifying him, and classifying him as a threat to society is functionally a prison.[62] Building on philosopher Jeremy Bentham's concept of the Panopticon—a prison where the inmates are cowed into self-regulation because they never know when they are being watched[63]—Foucault concluded that modern

---

of purchasing tickets, the amount of luggage, the appearance of nervousness, and the presence or absence of travel companions. *Id.* at 1011–12.

[56] Brief of Plaintiff at 31, Fazaga v. FBI, No. SACV11-00301 (C.D. Cal. Feb. 22, 2011) (class action complaint alleging that FBI agents "on several occasions talked about different individuals [mosque attendees] that they believed might be susceptible to rumors about their sexual orientation, so that they could be persuaded to become informants . . . .").

[57] The dignity and control of access interests are classified as such in Judith DeCew, *Privacy*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta, ed. Fall 2002, rev. 2008), *available at* http://plato.stanford.edu/entries/privacy.

[58] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964).

[59] DeCew, *supra* note 57 (citing Bloustein, *supra* note 58).

[60] DeCew, *supra* note 57 (citing ANITA ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988)).

[61] *Id.*

[62] MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 196–97 (1977).

[63] *Id.* at 198–99.

surveillance causes citizens to moderate their public behavior.[64] If surveillance were to saturate public life, the result would be "an interrogation without end,"[65] a society-wide panopticon. A common extension of this thesis is that people's awareness of surveillance causes them to forego not only illicit conduct but also legitimate conduct.[66] When citizens behave with the goal of appearing unimpeachable to authorities, their suppression of lawful acts endangers healthy dissent, nonconformity, and iconoclasm.[67] This liberty-endangerment will always lurk in the background of any court's analysis of FRT and the Fourth Amendment.

III. WHEN THE GOVERNMENT IDENTIFIES YOU BY YOUR FACE: SEARCH-AND-SEIZURE IMPLICATIONS

Given the privacy and liberty interests at stake, will FRT's use as a tool of the state be checked by the Fourth Amendment's prohibition on unreasonable searches and seizures?[68] Courts have not yet addressed the issue, but this Part finds that FRT occupies the vanguard in several search-and-seizure issues. FRT challenges will thus expose major fault lines in contemporary Fourth-Amendment jurisprudence, forcing courts to choose one side of the divide.

The Fourth Amendment's protection of privacy was defined in the 1967 case *Katz v. United States*, which held that the FBI's tapping of a public phone booth was an unconstitutional search.[69] The most widely-cited opinion in *Katz* is Justice Harlan's concurrence, which explained that a "search" occurs only when the suspect had a reasonable subjective expectation of privacy in the discovered material.[70] Harlan further stated that a search violates the Fourth Amendment only if society ratifies the person's expectations as objectively reasonable.[71] Armed with this two-part test, federal courts have generally held that people lack a subjective expectation of privacy in matters that they expose to the public, even to a very narrow segment of that public. When people throw out their trash,[72] cash checks at banks,[73] or drop off film for development,[74] they

[64] *Id.* at 207–08.

[65] *Id.* at 213.

[66] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260–61 (1998).

[67] *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

[68] The Fourth Amendment reads in part, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV.

[69] Katz v. United States, 389 U.S. 347, 353–56 (1967).

[70] *Id.* at 360 (Harlan, J., concurring).

[71] *Id.*

[72] California v. Greenwood, 486 U.S. 35, 43 (1988) (garbage left in public is accessible to any passerby and so is no longer the private property of its former owner).

[73] United States v. Miller, 425 U.S. 435, 436 (1976) (depositor's disclosure of the checks was voluntary and so waived expectation of privacy) (subsequently mooted in part by the Right to Financial Privacy Act, 12 U.S.C.S. § 3401 (MB)).

[74] Wabun-Inini v. Sessions, 900 F.2d 1234, 1239 (8th Cir. 1990) (even though customer did not expect photo developer to give customer's film to an FBI agent, the customer's handing the film to the developer waived his privacy rights), *en banc rehearing denied*, 1990 U.S. App. LEXIS 9520 (June 1, 1990).

effectively cede any expectation of privacy in those items by publicizing them to third parties.

Legal scholars have criticized the reasonable expectation test for exerting "a one-way ratchet against privacy"[75] rights. As technology continues to enhance government's power to monitor the public square, citizens' expectations of shielding information from the state's view necessarily diminishes.[76] Today, air travelers may feel invaded by airport body scanners that display images of the naked traveler to security officers; however, so long as travelers endure the process, the Fourth Amendment is not implicated.[77] Seen this way, Harlan's test sets no limit on how much the government can erode our access to secrecy and anonymity while moving outside the home.[78] Advocates of law enforcement discretion cheer at the prospect of a more-monitored public space, arguing that expectations of anonymity or secrecy facilitate criminal behavior and should be abrogated.[79] Regardless of ideology, scholars agree that advances in surveillance could soon winnow Fourth Amendment protection in public to a nub, if the reasonable expectation test continues to be literally applied.[80] This risk that technology will "outflank"[81] the search-and-seizure clause is no more salient than in the face-recognition context.

---

[75] Jim Harper, *Left Out in the Cold? The Chilling of Speech, Association, and the Press in Post-9/11 America: Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U.L. REV. 1381, 1382 (2008). *See also* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1306 (2002) (Harlan's test has effected "a gradual weakening of Fourth Amendment protections as investigative technologies become more sophisticated."). Thomas K. Clancy describes the problem this way: "permitting technological advances to reduce a person's protected interest inextricably leads to a smaller and smaller oasis of protection afforded by the Amendment." Thomas K. Clancy, *Coping with Technological Change:* Kyllo *and the Proper Analytical Structure to Measure the Scope of Fourth Amendment Rights*, 72 MISS. L.J. 525, 535 (2002).

[76] Jed Rubenfeld indicts the Harlan test's "prospective self-validation" with a simple illustration: "Suppose the President announces that all telephone conversations will henceforth be monitored. Arguably, no one thereafter can reasonably expect privacy in his phone calls, and the announced eavesdropping will have constitutionalized itself." Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 106 (2008). *See also* Harper, *supra* note 75, at 1392 ("If proponents of government surveillance can mold expectations to their advantage, they can have broad access to communications."); Simmons, *supra* note 75, at 1313 (citing Justice John Marshall's dissent in *Smith v. Maryland* that police could too easily "put the public on notice of the [privacy] risks" of new surveillance technology and thereby defeat the Harlan test).

[77] *See* Harper, *supra* note 75 at 1396.

[78] The courts have established a fairly bright-line rule that one's expectation of privacy inside the home is per se reasonable. *See* Thomas K. Clancy, *What is a "Search" Within the Meaning of the Fourth Amendment?* 70 ALB. L. REV. 1, 7–8 (2006).

[79] Breinholt, *supra* note 43, at 283 (concluding that "[o]ur expectations have evolved, with the help of technology" and criticizing concerns about loss of privacy in public as "eccentric[]" and "Luddite beliefs").

[80] *See* Tracey Maclin, Katz, Kyllo*, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 85–86 (2002) (if surveillance technology does not implicate Fourth Amendment protections simply because the surveillance occurs in public, the Fourth Amendment has effectively ceased operating in public places); Nguyen, *supra* note 4, at n.81 (citing T. Wade McKnight, *Passive, Sensory-Enhanced Searches: Shifting the Fourth Amendment "Reasonableness" Burden*, 59 LA. L. REV. 1243, 1260 (1999) (the race against privacy-eroding technology is "a race that the people will surely lose")). Thomas Clancy has commented that "technology will soon have the capability of making virtually everything knowable. Whether or when that increased ability is . . . a search under the Fourth Amendment is the core consideration of the twenty-first century." Clancy, *supra* note 78, at 30–31.

[81] Nguyen, *supra* note 4.

A. Is a Single Facial Identification in Public a Search?

A pedestrian passes a lamppost camera equipped with FRT and is unwittingly matched with his photo in a government database. Has a search occurred? If the situation is analogous to traditional surveillance techniques, the answer is a resounding no.

1. FRT as Analogous to Conventional Surveillance

When people exit their homes, they risk being observed by others and thereby forego any reasonable expectation of not being captured by surveillance, even if they believe they are not observed by anyone.[82] The case of Edward Kowalski illustrates the point.[83] Mr. Kowalski suffered a neck injury while working for the Pennsylvania State Police and, a few months after filing for workers' compensation, took a vacation to Florida.[84] While at the beach with his wife, he was unknowingly videotaped for days by a private investigator, hired by the State Police to verify Mr. Kowalski's medical condition.[85] Though most people would not expect or want to be surreptitiously recorded while sunbathing, Mr. Kowalski had no expectation of privacy and therefore no Fourth Amendment claim against the State Police.[86] This doctrine extends even to secluded spaces such as the elevators and hallways of commercial buildings, where recessed cameras often record goings-on.[87] Government agencies have a strong argument, then, that where people lack an expectation of not being *observed*, they equally lack an expectation of not being *recognized*. Because one could unexpectedly be recognized by a fellow pedestrian, so would go the argument, one cannot expect that FRT-equipped cameras will not match one's face against a government photobase.

This reasoning may strike some as strained, but it is the analysis that the Supreme Court has applied to surveillance since 1986, when *California v. Ciraolo* and *Dow Chemical Co. v. United States* were decided on the same day.[88] The cases presented similar facts. In *Ciraolo*, police officers flew an airplane 1,000 feet over a suspect's fenced-off property and observed a small marijuana field.[89] In *Dow Chemical*, EPA agents photographed the company's property from varying altitudes with a "precision aerial mapping camera."[90] Because the evidence gathering in both cases occurred from public airspace, the Court reasoned, any air traveler could have observed what the

[82] *See* United States v. Jackson, 213 F.3d 1269, 1280–81 (10th Cir. 2000) (surveillance by mounted cameras was not a search when it captured only what occurred outside suspect's home); United States v. Kim, 415 F. Supp. 1252, 1258 (D. Haw. 1976).

[83] Kowalski v. Scott, No. 02-7197, 2004 U.S. Dist. LEXIS 9935 (E.D. Penn. May 26, 2004).

[84] *Id.* at *3–*4.

[85] *Id.* at *4.

[86] *Id.* at *16.

[87] Adler, *supra* note 18, at *33 (citing *United States v. Vega*, 309 F. Supp. 2d 609, 613 (S.D.N.Y. 2004)).

[88] California v. Ciraolo, 476 U.S. 207 (1986); Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

[89] *Ciraolo*, 476 U.S. at 209.

[90] *Dow Chemical*, 476 U.S. at 229.

government agents did, had they bothered to look down.[91] EPA's reliance on a sophisticated camera did not amount to a search, said the Court, because: (1) the camera was available for public use,[92] and (2) the agents used the camera only to augment their natural sensory abilities.[93] The first fact matters because, if aerial mapping cameras are available in commerce, Dow could not have expected its land to be immune from the technology.[94] The second fact reflects the Court's view that, as long as technology does not give police novel powers of perception—the ability to see through walls or hear private conversations[95]—sensory-enhancing tools are not offensive to public expectations.[96]

Based on the example of *Dow*, police are able to enhance their noses with drug-sniffing dogs[97] and enhance their eyes with telescopes and binoculars.[98] Police cannot, however, aim a heat-sensing camera at a suspect's garage, since this technique is uncomfortably analogous to looking through a wall into a private space.[99] Still, as Justice Powell admonished in his *Dow* dissent, the "availability" and "sensory enhancement" tests inevitably abrogate public privacy as snooping technology becomes more pervasive.[100]

Linking surveillance cameras to FRT, then, arguably only enhances the police's already-existing senses: many surveillance advocates posit that scanning a face with FRT is simply a highly efficient version of looking through a traditional mug shot book.[101] Further support comes from cases where the police have sought to subpoena a suspect's handwriting or voice sample without a warrant. Because a person's handwriting and speech are frequently made public, the Court upholds such subpoenas, even though the

---

[91] *Ciraolo*, 476 U.S. at 213–14; *Dow Chemical*, 476 U.S. at 238–39.

[92] *Dow Chemical*, 476 U.S. at 238.

[93] *Id.* at 238–39.

[94] *See* Nicole Jacoby, *Redefining the Right to be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States*, 35 GA. J. INT'L & COMP. L. 433, 451 (2007); *But see* Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1395–96 (2002) (arguing that technological availability should be irrelevant to Fourth Amendment inquiry).

[95] *Dow Chemical*, 476 U.S. at 238; *See also* Katz v. United States, 389 U.S. 347, 356 (1967).

[96] *Dow Chemical*, 476 U.S. at 238–39.

[97] *See* United States v. Ludwig, 10 F.3d 1523, 1527 (10th Cir. 1993); Illinois v. Caballes, 543 U.S. 405, 409 (2005).

[98] *See* United States v. Kim, 415 F. Supp. 1252, 1254, 1258 (D. Haw. 1976). *See also* Florida v. Riley, 488 U.S. 445, 447-451 (1989) (holding that a observations with the naked eye, aided by the vantage point from a helicopter, does not constitute a "search" subject to the Fourth Amendment).

[99] Kyllo v. United States, 533 U.S. 27, 36–38 (2001).

[100] Justice Powell in his separate opinion in *Dow* warned against pegging Fourth Amendment protection to the availability of the particular technology, lest the dissemination of technology blunt Fourth Amendment protection. *Dow Chemical*, 476 U.S. at 251 (Powell, J., concurring in part and dissenting in part).

[101] DENNIS BAILEY, THE OPEN SOCIETY PARADOX: WHY THE 21ST CENTURY CALLS FOR MORE OPENNESS—NOT LESS 92 (2004); DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 313 (2003) (citing the Tampa Police Department's justifications for enhancing its street surveillance with FRT provided by the company FaceIt); J. K. PETERSEN, UNDERSTANDING SURVEILLANCE TECHNOLOGIES: SPY DEVICES, PRIVACY, HISTORY & APPLICATIONS 747 (2007) (citing Fairfax County, Virginia, police rationales for compiling arrestee mug shots into an FRT database).

requested sample is for the unusual purpose of *matching* the suspect's writing or speech to that of a criminal.[102] The pro-FRT interpretation is that, just as the government can demand a voice recording for matching purposes, so too can the government digitize a pedestrian's likeness for processing with a face-matching algorithm. As the Court stated in dictum in *United States v. Dionisio*, "No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world."[103] Though these cases were not decided in the surveillance context and so would not bind an FRT dispute, they foreshadow the Court's low-ebbing protection of facial privacy.

Nevertheless, challengers to FRT should engage the Harlan standard head-on by demonstrating that Americans reasonably expect *not* to be identified in public by sophisticated algorithms. Indeed, the Court has at times cast itself as a bulwark against novel technology that takes away privacies we once took for granted.[104] As evidence that people expect a degree of anonymity while moving in public, civil libertarians could point to the popular outcries that often accompany a city's installation of face-recognizing cameras.[105] Public reaction to Tampa Bay's use of FRT at the Super Bowl was overwhelmingly negative;[106] the subsequent installation of FRT cameras in Tampa's nightlife district prompted vociferous protests, effectively ending the city's FRT experiment two years later.[107]

Courts may respond that a person's outrage means nothing at the point at which surveillance technology meets the *Dow* test. This argument, made by lower courts in other contexts, is that as long as people know a technology could *conceivably* be used against them by strangers, the government's use of the technology is not a constitutional issue.[108] As articulated in one district opinion, "The proper inquiry . . . is not what a

---

[102] United States v. Mara, 410 U.S. 19, 21–22 (1973) (citing *United States v. Doe (Schwartz)*, 457 F.2d 895, 898–99 (2d Cir. 1972); *Bradford v. United States*, 413 F.2d 467, 471–72 (5th Cir. 1969); *Gilbert v. California*, 388 U.S. 263, 266–67 (1967)).

[103] Nguyen, *supra* note 4, at n.91 (citing *United States v. Dionisio*, 410 U.S. 1, 14 (1973)).

[104] As the Court warned in *Lopez v. United States*, "the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual . . . ." Lopez v. United States, 373 U.S. 427, 441 (1963).

[105] GLEE HARRAH CADY & PAT MCGREGOR, PROTECT YOUR DIGITAL PRIVACY: SURVIVAL SKILLS FOR THE INFORMATION AGE 174 (2002) (suggesting that widespread negative public opinion of face-recognizing techniques may be powerful evidence in civil liberties challenges).

[106] ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), PRIVACY AND HUMAN RIGHTS 2002: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 56 (2002); Kathryn Balint, *No "Snooper Bowl" for San Diego: Police Won't Be Using Face-Scanning Technology That Sparked Ire in Tampa*, SAN DIEGO UNION-TRIB., Jan. 20, 2003, at E1.

[107] Eggers, *supra* note 11, at 198. The security-technology company that installed Tampa's system, Graphco, was "pilloried by critics sounding the Big Brother alarm . . . ." Graphco also equipped the Salt Lake Winter Olympics' surveillance network with FRT, though the technology was not used during the event. Feder, *supra* note 28.

[108] *See infra* notes 173-177 and accompanying text (discussing *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007); *United States v. Burton*, 698 F. Supp. 2d 1303 (N.D. Fla. 2010); *In re Application of the United States of America for and Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and other Information; and (3) Authorizing the Disclosure of Location-Based Services* [hereinafter *CSLI: Austin*], 727 F. Supp. 2d 571 (W.D. Tex. 2010); *In re Application of the United States of America for an Order Directing a Provider of Electronic*

random stranger would actually or likely do [with surveillance technology], but rather what he feasibly could."[109] Members of the public could conceivably use an online FRT program such as Polar Rose to identify strangers on the street based on a furtively-snapped digital photo.[110] Making such a scenario all the more plausible, Google is now building an application that would locate a person's online Google Profile based on any photo of the person's face.[111] Thus, like it or not, under a strict reading of the *Dow* line, pedestrians have relinquished their expectation of facial-identity privacy.

Against this mechanical reading, however, a small revolt is stirring. In August 2010, the D.C. Circuit in *United States v. Maynard* held that police could not track suspects via their cell phone records without a warrant.[112] The holding was despite the government's truthful argument that a cell phone company could easily track any subscriber's movements by cataloguing the cell phone towers that received the subscriber's signal.[113] *Maynard* reviewed the Court's important "reasonable expectation" cases[114] and concluded: "In considering whether something is 'exposed' to the public . . . we ask not what another person can physically and may lawfully do but rather what a reasonable person *expects another might actually do*."[115] Were the D.C. Circuit to review state-run FRT, the inquiry would then be whether D.C. pedestrians expect their fellow travelers to discover their identities via FRT software. Three weeks after *Maynard*, a district court followed its result, emboldened by "several rulings in recent years" that reclaim domains of personal privacy threatened by encroaching technology.[116] Though the *Maynard* reasoning is for now the minority view,[117] it reflects a broadly felt instinct to reclaim the reasonable expectation test as a guardian of Fourth Amendment rights in public spaces.[118] Face-recognition challenges offer the potential to push *Maynard* further into the mainstream.

Communication Service to Disclose Records to the Government [hereinafter *CSLI: 3d Cir.*], 620 F.3d 304 (3d Cir. 2010)).

[109] United States v. Sparks, No. 10-10067-WGY, 2010 U.S. Dist. LEXIS 120257, at *18 (D. Mass Nov. 10, 2010).

[110] *See supra* notes 20-22 and accompanying text.

[111] Google users would have to opt into the application for their Profile information to be publicized in this way. *Google to Launch Facial Recognition Mobile App*, INT'L BUS. TIMES, Apr. 6, 2011, *available at* http://uk.ibtimes.com/articles/131041/20110406/google-face-recognition-app.htm. Google's face-recognition work is a small component of the company's wider development of algorithms capable of "quickly identify[ing] particular things or people from among vast stores of video and images . . . ." Rivka Galchen, *Dream Machine: The Mind-Expanding World of Quantum Computing*, THE NEW YORKER, May 2, 2011, at 39.

[112] United States v. Maynard, 615 F.3d 544, 555–56 (D.C. Cir. 2010).

[113] *Id.* at 559.

[114] *Id.* at 559–60. A notable reference in *Maynard* was to *Bond v. United States*, which found a police officer's squeezing of a bus passenger's luggage an unconstitutional search. Bond v. United States, 529 U.S. 334, 338–39 (2000). The *Bond* Court admitted that, while a bus passenger knows that a fellow traveler could squeeze his bag, an expectation to the contrary is reasonable. *Id.*

[115] *Maynard*, 615 F.3d at 559 (emphasis added).

[116] *In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information [Hereinafter *CSLI: NY*], No. 10-MJ-0550 (JO), 2010 U.S. Dist. LEXIS 88781, at *12 (E.D.N.Y. Aug. 27, 2010).

[117] *See supra* cases cited in notes 108-109.

[118] A sense of relief is detectable in *CSLI: NY* as the court cites Justice Kozinski's dissent in *United States v. Pineda-Moreno*, No. 08-30385, 2010 WL 3169573, at *7 (9th Cir. 2010) (Kozinski, C.J.,

2. The Dragnet Problem and the Analogy to Stop-and-Question Cases

Criticism of face-based surveillance often indicts the dragnet style with which all passersby are captured and identified.[119] Yet FRT's indiscriminate nature does not make it more search-like. Granted, our courts do not tolerate police dragnets used for gathering evidence of criminal wrongdoing,[120] such as roving immigration patrols,[121] highway drug-search checkpoints,[122] or hospitals that drug-test all pregnant patients.[123] Note, however, that no suspicionless investigation has ever been struck down unless it involved the physical search of a person or his secluded property. As Professor Thomas Clancy explains, this rule is likely due to the Court's deference to the Eighteenth-Century preoccupation with general warrants that inspired the Fourth Amendment's drafting.[124] Because "[t]he abhorred English and colonial search and seizure practices involved physical invasions," today's courts invalidate blanket surveillance only if it stops a person or snoops in a private space.[125] If FRT is to be invalidated under a "dragnet" theory, the identification would have to be analogous to a personal seizure.

In some respects, state use of FRT resembles a police practice that the Supreme Court considers an unreasonable seizure: where police stop a pedestrian without individualized suspicion and force him to answer questions.[126] In the 1979 case *Brown v. Texas*,[127] officers stopped a man on the street because (1) the area was known for drug trafficking, (2) the man was unfamiliar to the officers, and (3) the man had walked away

---

dissenting) ("There is something creepy and un-American about such clandestine and underhanded [continuous surveillance]. . . . Some day, soon, we may wake up and find we're living in Oceania"). *CSLI: NY*, 2010 U.S. Dist. LEXIS 88781, at *13.

[119] Milligan, *supra* note 19, at 320; Murphy, *supra* note 29, at 1393; Eggers, *supra* note 11, at 198 (quoting Gregory Nojeim of the ACLU as stating of public FRT, "Merely by walking down the street, a person is in essence put into an electronic police lineup without even knowing it.").

[120] *See* Robert C. Power, *Technology and the Fourth Amendment: A Proposed Formulation for Visual Searches*, 80 J. CRIM. L. & CRIMINOLOGY 1, n.270 (1989) (listing opinions that criticized or limited dragnet-style searches). By contrast, a highway roadblock that checks drivers for symptoms of drunkenness is not an unreasonable seizure, because its primary purpose is not to prosecute crimes but to curb the epidemic of drunk-driving fatalities. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 448–49 (1990).

[121] Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973) (though only twenty miles from the U.S.-Mexican border, the random halting of vehicles without individualized suspicion was an unreasonable seizure); United States v. Ortiz, 422 U.S. 891, 896–97 (1975) (even fixed checkpoints that search all cars for illegal immigrants are unreasonable if miles removed from the U.S.-Mexico border).

[122] City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000) ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing."). Even dog-sniffing a car without a warrant is constitutional *only* as an incident to an already-lawful traffic stop. *See* Illinois v. Caballes, 543 U.S. 405, at 409 (2005).

[123] Ferguson v. City of Charleston, 532 U.S. 67, 79–81 (2001) (declining to allow the blanket drug-testing of patients under the "special needs" doctrine).

[124] Clancy, *supra* note 78, at 4 (the "historical context" that motivated the search-and-seizure clause "has been viewed as a primary source for understanding the Amendment").

[125] *Id.* (emphasis added).

[126] Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697, 715 (2004) (people in public cannot be seized by police to coerce them into identifying themselves, unless the seizure was independently lawful).

[127] Brown v. Texas, 443 U.S. 47 (1979).

from another person.[128] When the man refused to give his name to the officers, he was arrested.[129] The arrest was unreasonable, the Court held, because it subjected civilians to "arbitrary invasions solely at the unfettered discretion of officers in the field."[130] Yet as subsequent Courts have mulled over *Brown*'s meaning, they have not signaled whether the violation stemmed from the forced *identification* of Brown, or the forced *stopping* of Brown. If the former, then FRT is a species of seizure, because it virtually coerces a pedestrian to identify himself;[131] if the latter, FRT is not limited by *Brown*, because it never delays the pedestrian's locomotion.[132]

Advocates of public FRT will point to *United States v. Mendenhall*[133] and *INS v. Delgado*[134] for the proposition that suspicionless identification is not a seizure unless the identified person is physically halted.[135] *Mendenhall* described a situation where DEA agents approached an air traveler who fit a "drug courier profile"[136] and asked for her ticket and identification;[137] *Delgado* dealt with an INS raid on a factory, during which some agents stood at the exits while others combed the factory floor inquiring into the workers' immigration statuses.[138] Both practices were upheld, and the opinions' holdings suggest that the decisive fact was the absence of physical detention: "We adhere to the view," wrote Justice Stewart in *Mendenhall*, "that a person is 'seized' only when, by means of physical force or a show of authority, his freedom of movement is restrained."[139] FRT's failure to detain the subject, then, probably places the technology outside the Court's seizure doctrine, a conclusion galvanized by *Delgado*'s statement that "a request for identification by the police does not, by itself, constitute a *Fourth Amendment* seizure."[140] The Court reasoned that an air traveler approached by DEA agents could conceivably ignore the agents and walk away,[141] and that factory workers could brush off the presence of INS agents and go about their business.[142] Though this

[128] *Id.* at 48. Scholarship has interpreted this fact pattern as insufficient to justify a forced stop, without more individualized suspicion. *See* Margaret Raymond, *Down on the Corner, Out in the Street: Considering the Character of the Neighborhood in Evaluating Reasonable Suspicion*, 60 OHIO ST. L.J. 99, 112–14 (1999).

[129] *Brown*, 443 U.S. at 49.

[130] *Id.* at 51.

[131] Steinbock, *supra* note 126, at 715–16; Nguyen, *supra* note 4, at VI.B.

[132] Tracey Maclin, *The Decline of the Right of Locomotion: The Fourth Amendment on the Streets*, 75 CORNELL L. REV. 1258, 1269 (1990) (interpreting caselaw as holding that a seizure has not taken place until the police arrest a person's locomotion).

[133] United States v. Mendenhall, 446 U.S. 544 (1980).

[134] INS v. Delgado, 466 U.S. 210 (1984).

[135] Clancy, *supra* note 78, at 37 ("in deciding whether the use of technology or senses other than the sense of touch should be labeled a search, the Court has sometimes" inquired whether the tactic is like a "physical invasion[]").

[136] For an explanation of a "drug courier profile," see *supra* note 55.

[137] *Mendenhall*, 446 U.S. at 547–48.

[138] *Delgado*, 466 U.S. at 212–13.

[139] *Mendenhall*, 446 U.S. at 553.

[140] *Delgado*, 466 U.S. at 216 (emphasis in original).

[141] *Mendenhall*, 446 U.S. at 554 ("[N]othing in the record suggests that the respondent had any objective reason to believe that she was not free to end the conversation in the concourse and proceed on her way.").

[142] *Delgado*, 466 U.S. at 216–17 (arguing that, while most civilians questioned by police obediently stop and respond, this does not mean they experience a lack of choice).

assumption has been ridiculed by scholars as utterly ignoring the power dynamic of police-civilian encounters,[143] it suggests that FRT's passivity ensures its Fourth Amendment compliance.

Read pragmatically, however, the stop-and-question decisions were written when the government was physically unable to check someone's identification without stopping him. FRT changes that, and civil libertarians could argue that what truly animated *Brown*, *Mendenhall*, and *Delgado* was the concern that people would have no choice in whether to identify themselves to police. According to Justice Stewart, when a random citizen makes a statement to police, the constitutional question is "whether it was made voluntarily,"[144] with no violation "[a]s long as the person to whom the questions are put remains free to disregard the questions . . . ."[145] *Delgado* too emphasized that when a person has no choice but to answer police questions, a seizure has occurred.[146] However, the only such scenario that Justice Rehnquist could imagine in 1984 was where "the circumstances of the encounter are so intimidating as to demonstrate that a reasonable person would have believed he was not free to leave if he had not responded . . . ."[147] FRT elides the need for such an intimidating atmosphere: by stepping in front of a face-identifying camera, a civilian is matched not only with his state-owned photograph but also any data associated with his name—residence, welfare status, employment, social security number, tax history, criminal record, child support compliance, etcetera. This new reality could urge courts to implicate *Brown* wherever surveillance forces a civilian to surrender personal information that would otherwise have remained unknown but-for a physical stop.[148]

3. Diminished Expectations of Privacy and the Special Needs Doctrine

Even if dragnet-style facial identification were determined a search or seizure, an FRT program that is more limited in scope or locale could survive a Fourth Amendment challenge. Limiting FRT photobases to a small class of highly suspect individuals may be allowed under the "diminished expectation" rule,[149] while FRT use only in highly sensitive locations would be exempt from Fourth Amendment scrutiny under the "special needs" doctrine.[150]

---

[143] Maclin, *supra* note 132, at 1298 ("[O]nly the most defiant citizens would feel free to leave a police officer under such circumstances.").

[144] *Mendenhall*, 446 U.S. at 556.

[145] *Id.* at 554.

[146] *Delgado*, 466 U.S. at 216–17.

[147] *Id.* at 216.

[148] This is based on Professor Clancy's proposed reform to search-and-seizure jurisprudence, which would protect "what any sense-enhancing device has discovered that would not have been discovered absent a physical invasion." Clancy, *supra* note 78, at 49.

[149] For a broad overview of the "diminished expectation of privacy" rule, see *Storing DNA Samples of Non-Convicted Persons & the Debate Over DNA Database Expansion*, 20 T.M. COOLEY L. REV. 509, 519–20 (2003).

[150] For a complete history of the "special needs" doctrine in U.S. jurisprudence, see Ric Simmons, *Searching for Terrorists: Why Public Safety Is Not a Special Need*, 59 DUKE L.J. 843, 850–84 (2010).

Courts have held for decades that certain classes of people, mostly students and convicts, have diminished expectations of privacy in certain matters. Whether a search of such persons violates that diminished expectation generally depends on three factors: (1) the person's relationship with the state,(2) the state's interest in obtaining the person's private information, and (3) whether that information is obtained in an unnecessarily intrusive way.[151] Thus, a school district can test a school athlete's urine for drugs because the school (1) has a supervisory role over the student,[152] (2) has a substantial interest in its prominent students' drug use,[153] and (3) uses the least intrusive testing method available.[154] Under similar reasoning, people convicted of felonies have a diminished expectation of privacy in their DNA samples,[155] and in the contents of their homes and cars.[156] By contrast, mere employees of the state retain their reasonable expectation of privacy in their bodies and so cannot be subjected to random urine testing.[157]

This rubric should allow a limited FRT program that uses only the photographs of parolees, fugitives, criminal suspects, and runaway minors, subject to the probable-cause requirements discussed in Part IV below. The state has a tightly regulated supervisory relationship with these classes, and the public's interest in locating them marginally outweighs the intrusion that a snapped photograph would cause.[158] Of course, such an FRT regime would still have to photograph every passerby, but if the passerby's face has no match in the FRT photobase, the file could be instantly discarded.[159] Such an intrusion into the passerby's privacy would thus be functionally the same as ordinary video surveillance, since the innocent passerby remains totally anonymous.[160] More troubling, however, is whether felons who have served their time could be photobased under the diminished expectation doctrine. Given the byzantine community-notification requirements for released sex offenders, a court would likely find that sex offenders' expectation of locational privacy is so low, the government can include them in FRT

[151] United States v. Knights, 534 U.S. 112, 119–20 (2001); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 654–58 (1995).

[152] *Acton*, 515 U.S. at 654. *See also* Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls, 536 U.S. 822, 830–32 (2002).

[153] *Acton*, 515 U.S. at 656. *See also Earls*, 536 U.S. at 834–38.

[154] *Acton*, 515 U.S. at 658. *See also Earls*, 536 U.S. at 832–34.

[155] *See* Banks v. United States, 490 F.3d 1178, 1193 (10th Cir. 2007); Johnson v. Quander, 440 F.3d 489, 491 (D.C. Cir. 2006); United States v. Weikert, 504 F.3d 1, 2–3 (1st Cir. 2007). However, jurisdictions are split over whether pre-trial detainees can be forced to supply DNA samples for databasing. *Compare* United States v. Pool, 621 F.3d 1213, 1214–15 (9th Cir. 2010) (allowing forced DNA sampling) *with* United States v. Mitchell, 681 F. Supp. 2d 597, 606–10 (W.D. Pa. 2009) (finding forced DNA sampling of pre-trial detainees an unreasonable search and seizure not subject to the "special needs" exception).

[156] *Knights*, 534 U.S. at 119–20.

[157] *See* Am. Fed'n of Teachers W.V., AFL-CIO v. Kanawha Cnty. Bd. of Educ., 592 F. Supp. 2d 883, 886 (S.D.W.V. 2009) (random drug testing of public school teachers is not reasonable); Capua v. City of Plainfield, 643 F. Supp. 1507, 1511 (D.N.J. 1986) (random drug testing of firefighters without pre-established standards is not reasonable).

[158] *See* Griffin v. Wisconsin, 483 U.S. 868, 870–73 (1987).

[159] Nguyen, *supra* note 4, at n.100.

[160] *Id.* See, however, *infra* Part V for a discussion of the probable-cause problems raised when an FRT system has a substantial false-positive rate.

photobases.[161] Ordinary felons, on the other hand, probably have the same interest in day-to-day locational privacy as anyone else; if the general public has a reasonable expectation in facial anonymity, a felon should have that expectation returned to him after parole.[162]

The government could also limit FRT use to buildings that are highly vulnerable to terrorist acts, thus avoiding Fourth Amendment inquiry under the special needs doctrine, which allows searches that are primarily for a purpose other than gathering evidence of criminality.[163] For example, in 2005 the Southern District of New York sanctioned random pat-downs in the New York Subway, because they are primarily for preventing bombings rather than conducting criminal investigations.[164] By analogy, facial identification is legitimate in places so vulnerable to attack that a fugitive or terrorism suspect must be nabbed immediately upon entry. Consistent with this use, DARPA has suggested that HumanID techniques would be concentrated on "large facilities," with the primary goal of intercepting attackers.[165] Still, for the government's interest in preventing terrorism to outweigh any evidence-gathering function of the search, the locale must truly be a credible terrorism target; commentary has noted that, because solid intelligence about terrorists' plans is scant, any public location could arguably be a "vulnerable" locale.[166] Tampa's enthusiasm for FRT exemplifies the slippery-slope problem. After successfully monitoring the 2001 Super Bowl (an arguable target) with FRT, the city expanded its FRT to ordinary city streets.[167] Unless courts demand evidence that a particular locale is more likely than others to be chosen for attack, the special needs doctrine could become the exception that swallows the rule.[168]

---

[161] *See* Caroline Louise Lewis, *The Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act: An Unconstitutional Deprivation of the Right to Privacy and Substantive Due Process*, 31 HARV. C.R.-C.L. L. REV. 89, 97–102 (1996).

[162] For the argument that even DNA databases should be limited to sex offenders and violent felons, see Mark A. Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 BROOK. L. REV. 127, 168–69 (2001).

[163] *See* Roberto Iraola, *DNA Dragnets – A Constitutional Catch?*, 54 DRAKE L. REV. 15, 24–25 (2005) (citing *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000) (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985))).

[164] MacWade v. Kelly, No. 05 Civ. 6921 (RMB) (FM), 2005 U.S. Dist. LEXIS 31281 (S.D.N.Y. Dec. 2, 2005). For analysis of the case, see *Recent Case: Second Circuit Holds New York City Subway Searches Constitutional Under Special Needs Doctrine* - MacWade v. Kelly, *460 F.3d 260 (2d Cir. 2006)*, 120 HARV. L. REV. 635 (2006).

[165] TIA REPORT, *supra* note 33, at 10–11.

[166] *Recent Case*, *supra* note 164, at 641 ("other cities with less extensive subway systems may find justification in MacWade for establishing their own search programs").

[167] *See supra* notes 106-107 and accompanying text.

[168] Blake Covington Norvell, *The Constitution and the NSA Warrantless Wiretapping Program: A Fourth Amendment Violation?*, 11 YALE J. L. & TECH. 228, 243–48 (2008-2009). For the argument that casting police officers as the front line against terrorism deteriorates Fourth Amendment protection, see Christopher Metzler, *Providing Material Support to Violate the Constitution: The USA PATRIOT Act and Its Assault on the 4th Amendment*, 29 N.C. CENT. L.J. 35, 61–63 (2006).

B. Would Cross-Referencing of Facial Identifications Create an Unreasonable Search?

Even if single facial identifications never implicated the Fourth Amendment, as is entirely possible,[169] the Amendment may restrain the state from storing FRT data and cross-referencing the identifications over time. In addition to the uses of cross-referencing described in Part II.B. above, cataloging identifications for long durations could also aid police in learning the associates of arrestees, identifying and locating witnesses to past crimes,[170] and confirming alibis.[171] Such practices go far beyond the single-identification use described in Part III.A. above, causing our locations to be known not only *at this moment* but for indefinite periods.

1. The Emerging Split over Long-Term Location Tracking

The district and circuit courts are currently struggling with a similar question—whether police can track suspects using either GPS locators or the suspects' cell phone records.[172] Some jurisdictions conclude that because a person has no privacy expectation in his individual movements, he has no privacy in his aggregated movements; police therefore can track his locations over time.[173] The basis for this argument is the Supreme Court opinion in *United States v. Knotts*, which permitted police to place a satellite-traced beeper in a drum of formaldehyde, and then follow the beeper's movement to a suspect's remote cabin.[174] The Court considered such activity functionally the same as "the following of an automobile on public streets," where the motorist has no expectation of privacy in his movement.[175] Subsequent courts have extended *Knotts* to any situation where a "device will track the person or object only in public places,"[176] paving the way for warrantless tracking of suspects' cars and cell phones. In these jurisdictions, FRT that stores and cross-references public identifications would violate no privacy expectations.[177]

---

[169] *See supra* Part III.A.

[170] In the treatise *Criminal Investigation*, Michael Palmiotto lists the major goals of surveillance, which include "verify the statement of a witness to a crime," "identify a suspect's associates," and "determine an informant's loyalty." MICHAEL PALMIOTTO, CRIMINAL INVESTIGATION 108 (2004). Such goals would be equally served by cataloging and cross-referencing facial identifications.

[171] The current lack of technical means to test alibis results in considerable subjectivity when factfinders consider alibi testimony in criminal trials. Dan Simon, *The Limited Diagnosticity of Criminal Trials*, 64 VAND. L. REV. 143, 170–73 (2011).

[172] For an overview of the arguments for and against requiring a warrant for cell-phone locational tracking, see Patrick T. Chamberlain, *Note: Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745 (2009).

[173] United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007); United States v. Burton, 698 F. Supp. 2d 1303, 1307-08 (N.D. Fla. 2010); *CSLI: 3d Cir.*, 620 F.3d 304, 312-13 (3d Cir. 2010); United States v. Sparks, No. 10-10067-WGY, 2010 U.S. Dist. LEXIS 120257, at *18 (D. Mass Nov. 10, 2010).

[174] United States v. Knotts, 460 U.S. 276, 281–83 (1983).

[175] *Id.* at 281.

[176] *CSLI: Austin*, 727 F. Supp. 2d 571, 577 (W.D. Tex. 2010).

[177] The *Garcia* court expressly compared GPS tracking to the aggregating of video surveillance data, stating that GPS tracking is no different from locating a car "by means of cameras mounted on lampposts . . . ." *Garcia*, 474 F.3d at 997.

Other courts, however, conclude the opposite: while a person has no privacy in a given public action, he reasonably expects privacy in the sum total of his public movements.[178] As recounted in Part III.A. above, the D.C. Circuit in *Maynard* recently held that simply because a motorist could be monitored 24 hours a day by GPS, he reasonably expects not being so tracked without a warrant.[179] According to the opinion, the chronicling of many days' movements generates an "intimate picture of [a person's] life," revealing "political, religious, amicable and amorous" relations.[180] Because "most Americans would be appalled by the notion that the Government could" chronicle their whereabouts without probable cause,[181] a warrant is required.[182] This reasoning is echoed in a cluster of cases requiring the government to show probable cause for cell-phone tracking.[183] Even courts that allow such monitoring have signaled that, if used on a massive and suspicionless basis, the technique could warrant Fourth Amendment scrutiny.[184]

2. Community Expectations of Locational Privacy

A challenge to long-term FRT monitoring would necessarily inquire into the social norms of locational privacy,[185] and there is ample evidence that Americans do not expect or want FRT to assemble rich, long-lasting personal profiles. In 2003, upon learning details of DARPA's Terrorism Information Awareness (TIA) program,[186]

---

[178] United States v. Maynard, 615 F.3d 544, 555-57 (D.C. Cir. 2010); *CSLI: NY*, No. 10-MJ-0550 (JO), 2010 U.S. Dist. LEXIS 88781, at *12 (E.D.N.Y. Aug. 27, 2010).

[179] *Maynard*, 615 F.3d at 555–57.

[180] *Id.* at 562 (quoting *People v. Weaver*, 12 N.Y.3d 433, 909 (N.Y. 2009)) (internal quotation marks omitted).

[181] *CSLI: Austin*, at 576 (quoting *In re Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government* [hereinafter *CSLI: Pittsburgh*], 534 F. Supp. 2d 585, 611 (W.D. Pa. 2008), *vacated*, *CSLI: 3d Cir.*, 620 F.3d at 319).

[182] *Maynard* noted that the *Knotts* Court expressly did not intend its holding to bind future analyses of "twenty-four -hour surveillance . . . ." *Maynard*, 615 F.3d at 556 (quoting United States v. Knotts, 460 U.S. 276, 283 (1983) (internal quotation marks omitted)).

[183] *In Re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 756–57 (S.D. Tex. 2005); *CSLI: Pittsburgh*, 534 F. Supp. 2d at 611, *vacated*, *CSLI: 3d Cir.*, 620 F.3d at 319; *CSLI: NY*, 736 F. Supp. 2d at 582.

[184] *See, e.g.*, *Knotts*, 460 U.S. at 284 ("if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable"); United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) ("One can imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns. . . . It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the Fourth Amendment.").

[185] Professor George C. Thomas and practitioner Barry S. Pollack observe that when the Court examines suspicionless checkpoint searches, the inquiry balances not only society's competing interests but also "what [intrusions] society is willing to accept." George C. Thomas III & Barry S. Pollack, *Saving Rights from a Remedy: A Societal View of the Fourth Amendment*, 73 B.U.L. REV. 147, 166 (1993). *See also* Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J. LAW & TECH. 319, 334–35 (2002) ("If American citizens remain entitled to value their privacy, they are the ones who have to decide how much of that privacy they might exchange for more security").

[186] *See supra* notes 34-39 and accompanying text.

Congress passed a resolution forbidding TIA's use against U.S. citizens residing in America, absent Congressional approval.[187] Scholars assert people's strong interest in attending public events that reveal their political or social sympathies without fear of being systematically recorded,[188] and government monitoring of political protests inevitably attracts scandal. When the Department of Defense instated "TALON," a program for gathering attendee information at anti-military gatherings, the press coverage was almost entirely hostile, and several Congresspersons called for public hearings into TALON's methods.[189] When the ACLU sued for an expedited FOIA request disclosing TALON files, a district court granted the request, holding that the public has a "compelling need" for the information, and that delay could "reasonably be foreseen to cause a significant adverse consequence to a recognized interest . . . ."[190]

A recent controversy at Apple illustrates the public's distaste for location-based data aggregation. In April 2011, security researchers discovered hidden code in the popular iPad and iPhone that stored the devices' "precise geographical location … marked with a timestamp."[191] The ensuing wave of negative press[192] prompted varying defenses from Apple, including: (a) geographic information sent to Apple is not as precise as that stored on the phone; (b) the data are "anonymized" rather than associated with the particular customer; (c) some of the software's location-tracking is caused by a "bug;" and (d) in the future, such data will be stored for no more than seven days.[193] Nonplussed by the company's statements, members of Congress pressed Apple executives to testify under oath on the issue, signaling a belief that their constituents value locational privacy.[194]

---

[187] Wyden, *supra* note 34, at 342.

[188] Sheri A. Alpert, *Privacy and Intelligent Highways: Finding the Right of Way*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 97, 105 (citing ROBERT BELAIR ET AL., PRIVACY IMPLICATION ARISING FROM INTELLIGENT VEHICLE HIGHWAY SYSTEMS 9 (1993)).

[189] *See* ACLU v. Dep't of Def., No: C 06-01698 WHA, 2006 U.S. Dist. LEXIS 36888, at *4–*8 (N.D. Cal. May 25, 2006).

[190] *Id.* at *15 (quoting *Al-Fayed v. CIA*, 254 F.3d 300, 310–11 (D.C. Cir. 2001)) (internal quotation marks omitted).

[191] David Sarno, *IPhone and iPad can track location of users; Researchers find a file in the Apple devices that can contain a detailed history over months or even years*, L.A. TIMES, Apr. 21, 2011, at B1.

[192] *See* Editorial, *Don't let technology get ahead of privacy*, CHI. SUN-TIMES, Apr. 22, 2011, at 20; Troy Wolverton, *iSpy: Apple's iPhones can track users' movements*, SAN JOSE MERCURY NEWS, Apr. 20, 2011 (quoting Center for Digital Democracy spokesperson that "[t]his is a crisis moment for Apple"); Alex Dickinson, *Privacy group ire for iPhone – Bad reception for Apple mobile devices that track user movements*, THE COURIER MAIL (Australia), Apr. 23, 2011, at 14; Chloe Albanesius, *Apple Sued Over iPhone Tracking*, PC MAGAZINE, Apr. 26, 2011 (describing class action suit filed against Apple in Florida district court); Jeremy Herb, *Calls fly over phones' tracking*, MINNEAPOLIS STAR TRIB., Apr. 23, 2011, at A1.

[193] Peter Pachal, *Apple Speaks Out on iPhone Tracking, Promises to Encrypt Location Data*, PC MAGAZINE, Apr. 27, 2011.

[194] *See* Chloe Abanesius, *How Do Third-Party Apps Handle Location Data? Congress Wants to Know*, PC MAGAZINE, Apr. 28, 2011; *I(Pad) Will Be Watching You*, BOS. HERALD, Apr. 22, 2011, at 18 (describing Representative Edward Markley's letter to Apple); Hayley Tsukayama, *Alarm on Hill over iPhone location tracking*, WASH. POST, Apr. 22, 2011, at A13 (reporting Representative Jay Inslee's call for protective legislation).

On the other hand, public anxiety over terrorism could cause Americans to see long-term locational privacy as a threat to security, rather than an interest worthy of protection. Professor Richard Sobel observes that before the 9/11 attacks a minority of Americans favored a mandatory national ID card, whereas 70% favored a national ID following the attacks.[195] Similarly, Jeff Breinholt, a staunch advocate of HumanID-type surveillance,[196] notes that there are two types of airport body-scanners: one that visualizes the human body as a blob, and the other that renders an accurate naked image.[197] Though the two are equally effective in detecting weapons, surveys indicate that much of the public would prefer the "naked" machines be installed at airports.[198] To Breinholt this is evidence that, while "it would seem that Americans care deeply about personal privacy and human dignity . . . they are more concerned about feeling safe . . . ."[199] It is also likely that, once exposed to a new privacy intrusion, the public rapidly adjusts its definition of human dignity to accommodate the intrusion.[200]

Nevertheless, primary sources from the federal government reveal that government attorneys probably regard the aggregation of personal data—particularly locational data—as compromising Fourth Amendment rights. As reported by *The New York Times*, Pentagon guidelines require the deletion of information about anti-military protesters "within three months if they [do] not pose a security threat."[201] Furthermore, in its TIA Report, DARPA was disarmingly upfront about the constitutional threats posed by HumanID and other tools. Among the "most important" privacy concerns the Report identified was:

> [a]ccess to aggregate individually identifiable information. Even when individual items of data are not particularly sensitive, access to an aggregation of significant quantities of personal data on specific persons represents opportunities for . . . unwarranted intrusion into personal matters.[202]

DARPA tacitly admitted that if a HumanID program causes surveillance tapes to be retained and analyzed for long periods, the government's Fourth Amendment position weakens markedly.[203] These sources could liberate federal courts to follow the *Maynard*

---

[195] Sobel, *supra* note 185, at 333, 377.

[196] *See supra* notes 43, 50, 79 and accompanying text.

[197] Breinholt, *supra* note 43, at 277.

[198] *Id;* Jeffrey Rosen, *The Way We Live Now: Essay: Naked Terror*, N.Y. Times, Jan. 4, 2004, at 10 (explaining some travelers' preference for a naked scanner and observing, "Some say they are already searched so thoroughly at airports that they have abandoned all hope of privacy. Others say those who have nothing to hide should have nothing to fear").

[199] Breinholt, *supra* note 43, at 277.

[200] Professor Sobel calls this process "acculturation." Sobel, *supra* note 185, at 333–34. Commentary also hypothesizes that when the public observes new security measures, the public is more likely to interpret the security as being necessary. *See* Milligan, *supra* note 19, at 325.

[201] ACLU v. Dep't of Def., No: C 06-01698 WHA, 2006 U.S. Dist. LEXIS 36888, at *4 (N.D. Cal. May 25, 2006) (citing David S. Cloud, *Pentagon Is Said to Mishandle a Counterterrorism Database*, N.Y. TIMES, Dec. 16, 2005, *available at* http://www.nytimes.com/2005/12/16/politics/16pentagon.html#).

[202] TIA REPORT, *supra* note 33, at 29 (emphasis in original).

[203] *See id.* at 35.

line and disallow warrantless aggregation of FRT data that draws an "intimate picture" of a subject's life.[204]

IV. BUILDING DATABASES OF FACIAL PHOTOGRAPHS: STATUTORY AND CONSTITUTIONAL LIMITS

For FRT to function, the state needs pre-labeled photographs of its citizens, and the gathering of these photographs may implicate federal law as well as the Fourth Amendment. Governments already have proprietary control over four major sources of facial photos: arrestee mug shots, passport photos, driver's license photos, and border-entry photos of non-citizens.[205] Agencies can be expected to exploit these resources to support FRT to the maximum extent allowed by law.

A. Statutory Limits: An Easy Workaround

States are generally free to compile lawfully-gathered information about their citizens,[206] so the states assembling mug shot and driver's license photobases are not acting improperly.[207] Federal photobasing capabilities, however, are limited by the Privacy Act of 1974.[208] The Act forbids one federal agency from sharing a person's private information with another agency[209] unless (1) the disclosure is for the same purpose for which the information was collected (the "routine use" exception)[210] or (2) the disclosure serves an authorized law enforcement activity.[211] Photobasing federal passport and border-entry pictures arguably fits neither of these exceptions. There is no "routine use," since the photos' original purpose was to administrate border crossings, not to track citizens within U.S. borders.[212] Regarding the law enforcement exception, the government could argue that assembling an FRT photobase is one general "law enforcement activity," but courts would almost certainly require a connection to a

[204] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

[205] Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 751–52 (1989); Cate, *supra* note 39, at 442; Ayelet Shachar, *The Shifting Border of Immigration Regulation*, 30 MICH. J. INT'L L. 809, 819–20 (2009); Liptak, *supra* note 31.

[206] *See, e.g.*, St. Michael's Convalescent Hosp. v. California, 643 F.2d 1369, 1373 (9th Cir. 1981) (affirming that Privacy Act of 1974 does not bind states).

[207] *See* Murphy, *supra* note 31, at 1342 and accompanying text.

[208] 5 U.S.C.S. § 552a et seq. (LexisNexis 2011).

[209] *Id.* § 552a(b).

[210] *Id.* § 552a(b)(3)

[211] *Id.* § 552a(b)(7). The Privacy Act contains other exceptions that are not relevant to this discussion. *See* Cate, *supra* note 39, at 465–66.

[212] For examples of inter-agency data-sharing that did not meet the routine use exception, see Cooper v. Fed. Aviation Admin., 596 F.3d 538 (9th Cir. 2010) (FAA could not obtain pilot's medical records from Social Security Administration to investigate suspected fraud); Stafford v. Soc. Sec. Admin., 437 F. Supp. 2d 1113 (N.D. Cal. 2006) (Social Security Administration cannot send plaintiff's mental health records to a state child protective services agency); Britt v. Naval Investigative Serv., 886 F.2d 544 (3d Cir. 1989) (NIS could not notify naval officer's new employer, the INS, about pending investigation into officer's conduct); Covert v. Herrington, 663 F. Supp. 577 (E.D. Wash. 1987) (personal information gathered by DOE for employee security clearance could not be used within the DOE for fraud investigation).

specific law enforcement operation for this exception to apply.[213] Massive photobasing to support future FRT lacks even a distant nexus with a particular criminal investigation and so would violate the Act.

Perhaps these limitations will not hinder federal FRT development: the FBI is currently populating a "massive database" [214] of information on anyone who has ever been arrested by state or federal officers, including mug shot photographs.[215] But what if the FBI or other agency seeks access to a broader class of photos—most notably from social networking sites such as Facebook? The Stored Communications Act of 1986[216] aspires to shield such data from federal snooping, but the statute has a prominent loophole. After a communication has been stored for 180 days, a federal agency can obtain it from the telecom provider merely with an administrative subpoena.[217] When written, the Act required the subpoena to aver that "specific and articulable facts"[218] made the requested material relevant to an ongoing criminal investigation.[219]

The USA PATRIOT Act further weakened the protection of stored communications by creating a new form of administrative subpoena—the National Security Letter,[220] or NSL. By sending an NSL to a telecom or ISP company, an agency can receive a wide scope of customer information without the "specific and articulable facts" requirement; the agency is asked only to certify that "information relevant to a terrorism investigation may be obtained."[221] That "may" caveat permits ISP user data to be collected in bulk without individualized suspicion, conditioned only on the agency's good-faith belief that the collection serves anti-terrorism goals.[222] Because NSLs usually contain clauses forbidding the recipient from disclosing receipt of the letter, the extent of communications collection by the federal government is unquantifiable.[223] Anecdotal reports, however, indicate that the major telecom firms have supplied bulk customer files even without administrative subpoenas;[224] Facebook receives upwards of ten to twenty

[213] The closest analogy is to the "law enforcement exception" of the Freedom of Information Act, whereby an agency may suppress records for a law enforcement purpose. Courts, however, require the suppression to be rationally connected to a specific law enforcement operation. *See* Berger v. IRS, 487 F. Supp. 2d 482 (D. N.J. 2007).

[214] Barr, *supra* note 44, at 1407.

[215] James Jacobs & Tamara Crepet, *The Expanding Scope, Use, and Availability of Criminal Records*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 177, 181–82 (2007-2008). Local police departments have long shared arrestee data with federal agencies on a voluntary basis. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 752 (1989).

[216] 18 U.S.C.S. §§ 2701–2711 (MB 2011).

[217] *Id.* § 2703(c)(2). For an interpreting case, see *United States v. Polizzi*, 549 F. Supp. 2d 308 (E.D.N.Y. 2008).

[218] *In re* United States Orders pursuant to 18 U.S.C. 2703(d), 509 F. Supp. 2d 76, 77 (D. Mass. 2007).

[219] *CSLI: 3d Cir.*, 620 F.3d 304, 309 (3d Cir. 2010).

[220] 18 U.S.C. § 2709(b) (MB 2011).

[221] Susan N. Herman, *The USA PATRIOT Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67, 87 (2006).

[222] *Id.*

[223] U.S. Internet Service Provider Assn., *Electronic Evidence Compliance - A Guide for Internet Service Providers*, 18 BERKELEY TECH. L.J. 945, 970–71 (2003).

[224] *See* Mary Swanton, *Divulging Data; Government request for customer records put companies in a tight spot*, INSIDE COUNSEL, at 18 (July 2006) (recounting that, even before receiving NSLs, three major telecom companies shared customer data with federal agencies).

non-NSL requests per day from government agencies, and likely many more NSLs that the company cannot discuss.[225] Statutory barriers, then, would apparently not stall the building of federal photobases, even of people who have never been accused of crimes.

B. Fourth Amendment Limits: An Area for Reform

Warrantless gathering of social-network photos exposes yet another Fourth Amendment fault line that threatens to rupture. In the majority view, when an internet user shares information with an ISP, the information becomes non-private and its disclosure to the government is a non-search.[226] This jurisprudence traces back to *Smith v. Maryland*, which allowed police to collect records of the phone numbers a suspect dialed from his home, on the theory that the suspect knowingly shared those numbers with the phone company.[227] The logic of *Smith* has been exported from the limited, analog world of phone numbers to the expansive digital terrain of the internet. Today, many courts would consider Facebook photos outside the Fourth Amendment's ambit;[228] even if the poster set his privacy settings to allow only friends to view the photos, he still necessarily shares those photos with Facebook itself, waiving his constitutional privacy expectations.[229]

A minority voice, however, intends to return some expectation of privacy to the individual in the digital world. Much like the small judicial backlash occurring against warrantless electronic tracking of suspects,[230] a few courts are crafting a newly robust vision of the average internet user's reasonable expectation of privacy. For years, scholars have commented that the third-party disclosure doctrine "makes little logical or practical sense" in the online communication context,[231] and recent opinions reflect that such illogic has a breaking point. According to the Ninth Circuit, a student who signs-on to a university's intranet retains a reasonable expectation of privacy in his computer files,

---

[225] Soghoian, *supra* note 49, at 394.

[226] Harper, *supra* note 75, at 1402 ("the government can compel a service provider to maintain records about a customer and then collect those records without implicating his or her Fourth Amendment rights"); Cate, *supra* note 39, at 454–55.

[227] Smith v. Maryland, 442 U.S. 735, 744 (1979) ("the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . even if the information is revealed 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") (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)).

[228] *See* Freedman v. America Online, Inc., 412 F. Supp. 2d 174, 181–82 (D. Conn. 2005) (citing *United States v. Hambrick*, 55 F. Supp. 2d 504 (W.D. Va. 1999); *United States v. Kennedy*, 81 F. Supp. 1103 (D. Kan. 2000)). *See also* United States v. King, 509 F.3d 1338, 1341–42 (11th Cir. 2007) (holding that a civilian contractor had no expectation of privacy when he inadvertently exposed laptop content to the military base's network).

[229] *See* Lisa Graves, *The Right to Privacy in Light of Presidents' Programs: What Project MINARET's Admissions Reveal about Modern Surveillance of Americans*, 88 TEX. L. REV. 1855, 1901 (2010). *See also* Joshua L. Simmons, *Note: Buying You: The Government's Use of Fourth-Parties to Launder Data About "the People"*, 2009 COLUM. BUS. L. REV. 950, 992–93, 999 (2009).

[230] United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010).

[231] Cate, *supra* note 39, at 455–56 (citing Professor Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089 (2002) ("[w]e are becoming a society of records, and these records are not held by us, but by third parties")).

even though university policy allows network administrators to view those files.[232] Extending this ruling, the Sixth Circuit in *United States v. Warshak* rejected a federal subpoena seeking customer email records from an ISP.[233] While the Electronic Stored Communication Act does not require probable cause for obtaining the subpoena,[234] *Warshak* admonished that the Fourth Amendment still requires probable cause if the ISP customer has a reasonable expectation of privacy in the matter sought.[235] The court held that an email is much more like the content of the phone conversation protected in *Katz*[236] than like the numbers the suspect dialed in *Smith*.[237] Acknowledging that an online customer knows his ISP could technically snoop on his emailing, the court found that customers expect their ISPs to respect basic social boundaries.[238] While perhaps misplaced, this faith of confidentiality erects a virtual fence around online communications, rendering state intrusion to be classified as a search.

Professor Orin Kerr has argued that at most the Fourth Amendment protects online "information that is sealed away from the network provider," a narrow class of communications limited mostly to the content of emails and documents.[239] Because social network photos are posted directly to the company's servers without the virtual "envelope" of an email, Kerr would consider such files non-private.[240] Yet *Warshak* interpreted its precedent more broadly, concluding that online posting enjoys protection if the poster intentionally limited the audience of the content;[241] this test is consistent with the earlier *United States v. Maxwell*, in which a military judge ruled that an online communication's private status hinged on whether it was disseminated to an indiscriminate public, as in a chat room, or to a select list of recipients.[242] Social network postings that the subscriber hides behind privacy settings should therefore follow *Warshak* and *Maxwell*. The *Warshak* reasoning has been eagerly extended by other jurists to protect cell-phone location records[243] and digits entered into a phone other than

[232] United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007).

[233] United States v. Warshak, 490 F.3d 455, 460, 475–76 (6th Cir. 2006) (*rev'd en banc on other grounds*, Warshak v. United States, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007)).

[234] *Id.* at 468.

[235] *Id.* at 469.

[236] *Id.* at 471 ("[l]ike telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course").

[237] *Id.* at 470–71 ("under *Katz*, the mere fact that a communication is shared with another person does not entirely erode all expectations of privacy, because otherwise eavesdropping would never amount to a search").

[238] *Id.* at 471.

[239] Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U.L. REV. 607, 628 (2003).

[240] *See id.* at 614–17, 627–28.

[241] *Warshak*, 490 F.3d at 472 (citing *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2007) ("the public disclosure of material to an untold number of readers distinguishes bulletin board postings from e-mails, which typically have a limited, select number of recipients")).

[242] United States v. Maxwell, 45 M.J. 406, 418–19 (C.A.A.F. 1996).

[243] *See* CSLI: NY, No. 10-MC-0897 (JO), 2010 U.S. Dist. LEXIS 136053, at *10–*12 (E.D.N.Y. Dec. 23, 2010); *CSLI: Pittsburgh*, *supra* note 181, at 587, 608–09, *vacated*, *CSLI: 3d Cir*, 620 F.3d at 319 (without *Warshak*-like expectations of privacy, Fourth Amendment protection of online communication would be "hollow").

phone numbers.[244] The nascent body of law asserting a customer's expectation of confidentiality when sharing data with a telecom firm could become a mainstream view if the government attempts to collect social network photos. As with other legal fault lines exposed by FRT, such collection would sound an alarm to American society about how vulnerable our public lives are becoming to arbitrary monitoring. This is yet another reason why state use of face-based surveillance could inspire newfound enthusiasm for Fourth Amendment principles.

V. FACE-RECOGNITION ALGORITHMS: A CHALLENGE FOR PROBABLE CAUSE

Whether identification by an FRT system establishes probable cause to search or detain a person is a final area where this technology will test the Fourth Amendment's meaning. As described in Part II above, FRT's failure rate varies widely according to the algorithms used,[245] number of facial features analyzed,[246] lighting conditions,[247] and duration of the surveillance clip.[248] In 2002 the National Institute of Standards and Technology determined that the best-performing FRT software experienced only a 1% false-positive rate indoors;[249] by contrast, Boston Logan's 2003 experiment with FRT generated false positives on more than 19% of its identifications.[250] When basing its matches on surveillance video, the average FRT algorithm errs an estimated 40% of the time, either misidentifying a subject or failing to make any identification.[251] Even today's most precise programs may show escalating failure rates over time, as stored photos cease to resemble the aging humans that the software is attempting to recognize.[252] Because false positives necessarily subject innocent civilians to unwarranted police scrutiny, courts and agencies must decide how accurate the Fourth Amendment requires an FRT system to be.[253]

---

[244] *In the Matter of Applications of the United States of America for Order (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information*, 515 F. Supp. 2d 325, 337–38 (E.D.N.Y. 2007). Even when distinguishing *Warshak*, courts acknowledge the decision's persuasiveness on the subject of online reasonable expectation of privacy. *See* United States v. D'Andrea, 497 F. Supp. 2d 117, 121–22 (D. Mass. 2007), *vacated*, United States v. D'Andrea, 648 F.3d 1 (1st Cir. 2011) (while the government may be prevented from hacking into a password-protected website without probable cause, private individuals with legitimate access to the site are free to pass on information to the authorities).

[245] *See supra* notes 6, 9, 16 and accompanying text.

[246] *See supra* note 5 and accompanying text.

[247] *See supra* note 14 and accompanying text.

[248] *See supra* note 15 and accompanying text.

[249] *See* PHILLIPS ET AL., *supra* note 9, at 8.

[250] *See* Wechsler, *supra* note 10, at 4 (reporting that the Logan system's failure rate was 38.6% and that more than half of those incorrect identifications were false positives).

[251] *See supra* note 12 and accompanying text.

[252] *See* Eric Patterson et al., *Automatic Representation of Adult Aging in Facial Images*, 2006, PROC. SIXTH IASTED INT'L CONF. ON VISUALIZATION, IMAGING, AND IMAGE PROCESSING 171, 171 (explaining that, when most FRT programs are tested for accuracy, little time has elapsed since the program's database photos were taken).

[253] The relevant clause provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation . . . ." U.S. CONST. amend. IV.

A. Tolerable Error and the "Fair Probability" Test

Illinois v. Gates[254] determined that probable cause is a "totality of the circumstances" standard, inquiring whether the information available to police objectively creates a "fair probability" that a search or seizure will yield evidence of criminality.[255] Law enforcement agents rely on diverse sources of intelligence when investigating cases,[256] but FRT belongs to a special class of sources that supply information independent of police judgment. This class includes expert testing,[257] canine drug-sniffs,[258] and to some extent confidential informants.[259] These sources are problematic for the Fourth Amendment because they prompt police to conduct searches and seizures with only a limited opportunity for independent evaluation of probable cause.[260] In these situations, therefore, courts focus on the source's reliability as the touchstone of Fourth Amendment compliance. Cases involving informants are instructive.[261] The great majority of federal courts have read *Gates* to allow searches and seizures based on a tip, where the tipster has supplied fruitful information in the past.[262] A sizable majority also find probable cause where the tip is supported simply by a police statement that the source is trustworthy.[263] If an algorithm is like an informant, then the

[254] Illinois v. Gates, 462 U.S. 213 (1983).

[255] *Id.* at 238.

[256] *See Investigations and Police Practices*, 38 GEO. L.J. ANN. REV. CRIM. PROC. 3, 15–19 (2009) (listing the four major categories of sources that prompt police searches and seizures).

[257] *See* Bruce L. Ottley, *Beyond the Crime Laboratory: The Admissibility of Unconfirmed Forensic Evidence in Arson Cases*, 36 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 263, 268–70 (2010) (describing attempts by arson investigators to measure objectively whether a fire was deliberately set); Alexandra J. Roberts, *Everything New is Old Again: Brain Fingerprinting and Evidentiary Analogy*, 9 YALE J.L. & TECH. 234, 256–57 (2006) (describing EEG brain-scanning of suspects to determine whether the suspect is concealing information relevant to an investigation).

[258] *See Investigations and Police Practices*, *supra* note 256, at n.33 (listing cases in which police relied on drug-sniffing dogs to gather evidence in anticipation of an arrest).

[259] Tips supplied by informants often do not result in arrests or searches until officers have independently and personally verified that aspects of the tip are accurate. *See Investigations and Police Practices*, *supra* note 256, at 16–17. However, a majority of federal courts allow warrants to issue simply based on indicia of an informant's *past* reliability. *See infra* notes 262–263 and accompanying text.

[260] The Supreme Court has ruled that magistrate judges, when issuing warrants, are entitled to defer to the professional judgment of police officers. United States v. Watson, 423 U.S. 411, 423 (1976). The importance of police judgment has led justices and commentators to wrestle with the question of how much an officer should corroborate an outside source's information before acting on it. *See* Yale Kamisar, Gates, *"Probable Cause," "Good Faith," and Beyond*, 69 IOWA L. REV. 551, 558–66 (1984).

[261] When a search is based on an informant's tip, *Gates* asks whether the informant's "reliability" and "basis of knowledge" objectively establish the "fair probability" that evidence of criminality will come to light. *See* Illinois v. Gates, 462 U.S. 213, 230 (1983).

[262] Brian Sheppard has compiled an exhaustive list of case notes applying *Gates* in the following American Law Report: Brian Sheppard, Annotation, *Sufficiency of Information Provided by Confidential Informant, Whose Identity Is Known to Police, to Provide Probable Cause for Federal Search Warrant Where There Was Indication That Informant Provided Reliable Information to Police in Past -- Cases Decided after* Illinois v. Gates, *462 U.S. 213, 103 S. CT. 2317, 76 L. ED. 2D 527 (1983)*, 196 A.L.R. FED. 1, at II.A.3, II.A.4b (2004) (finding only one federal opinion ruling that no probable cause existed where the tipster had formerly supplied information leading to the discovery of evidence).

[263] *Compare id.* at II.A.7a *with id.* at II.A.7b (finding only five federal opinions that have ruled against probable clause based on police statement of informant's past reliability). Because statements by informants are hearsay, federal rules and the Supreme Court require that police supply some evidence of

algorithm's identification of a pedestrian as a wanted suspect should be supported by past indicia of accuracy in order for the police to stop the pedestrian and check his ID, or take him to the station for fingerprinting.[264] But what is the tolerable rate of error?

The Supreme Court has long held that probable cause is not a preponderance-of-the-evidence standard,[265] and FRT enthusiasts have a strong argument that an FRT algorithm need only be right a substantial percentage of the time in order to establish probable cause for a search or seizure.[266] In support of this position, a majority of cases allow a drug-sniffing canine's behavior to trigger a search of private property, even where the dog's false-positive rate was known to be high[267] (nearly 50% in the more extreme cases[268]). Courts' attitudes about the usefulness of field sobriety tests are similarly permissive. Experts have noted that the Vertical and Horizontal Gaze Nystagmus Tests ("VGN" and "HGN" respectively), administered by specially-trained officers at traffic stops,[269] falsely indicate drug intoxication in about 23% of cases.[270] Nevertheless, only one court has ruled that this error rate precludes the officer from detaining a suspect who fails the test.[271] Thus, the case law suggests that a government agency may satisfy the probable cause standard without having to invest in the best-performing FRT available.

---

the informant's trustworthiness to obtain a search warrant. S. Bernstein, *Propriety of Considering Hearsay or Other Incompetent Evidence in Establishing Probable Cause for Issuance of Search Warrant*, 10 A.L.R.3d 359, at I.2b (2010).

[264] Transporting a suspect for fingerprinting is a species of detention that requires probable cause, rather than a mere reasonable suspicion of wrongdoing. Hayes v. Florida, 470 U.S. 811, 814–15 (following *Davis v. Mississippi*, 394 U.S. 721 (1969)).

[265] *Gates*, 462 U.S. at 235 (citing Locke v. United States, 7 Cranch 339, 348 (1813); Brinegar v. United States, 338 U.S. 160, 173 (1949)). *See also* Joseph D. Grano, *Probable Cause and Common Sense: A Reply to Critics of* Illinois v. Gates, 17 U. MICH. J.L. REFORM 465, 473–74 (1984) (the probable cause standard for searching a suspect, or detaining him long enough to secure more information, is lower than the standards for custodial arrest or the various evidentiary burdens of proof).

[266] Judges are entitled to grant search warrants where "*any set of facts* . . . support the accuracy of the information supplied by" a source. United States v. May, 399 F.3d 817, 824 (6th Cir. 2005) (citing Jones v. United States, 362 U.S. 257, 271–72 (1960)) (emphasis added).

[267] *See* United States v. Scott, 610 F.3d 1009, 1014 (8th Cir. 2010) (dog's 15% error rate in the field did not negate probable cause); United States v. Ohoro, 724 F. Supp. 2d 1191, 1203–04 (M.D. Ala. 2010) (citing unpublished decision finding a 45% error rate acceptable); United States v. Limares, 269 F.3d 794, 797 (7th Cir. 2001) (accepting a 38% failure rate as sufficient); United States v. Koon Chun Wu, 217 F. App'x 240, 246 (4th Cir. 2007) (dog's 40% failure rate did not negate probable cause). A handful of courts have set a higher bar for canine accuracy. *See* Commonwealth v. Ramos, 72 Mass. App. Ct. 773, 776 (App. Ct. Mass. 2008) (drug-alert by dog who had only five to six correct identifications and two false alerts in the past six months could not create probable cause); United States v. Huerta, 247 F. Supp. 2d 902, 910 (S.D. Ohio 2002) (drug-alert from dog with 65% accuracy rate was insufficient for probable cause).

[268] United States v. Donnelly, 475 F.3d 946, 955 (8th Cir. 2007) (46% inaccuracy rate did not negate probable cause where canine had been properly trained and handled).

[269] In administering the tests, an officer trained as a "Drug Recognition Expert" instructs a suspect to follow a moving object either vertically or horizontally with his eyes. The officer measures drug intoxication by the twitching movements of the suspect's eyeball. Jim Fraiser, Annotation, *Vertical Gaze Nystagmus Test: Use in Impaired Driving Prosecution*, 117 A.L.R.5th 491, at I.2a (2008).

[270] *See* United States v. Horn, 185 F. Supp. 2d 530, 537 (D. Md. 2002).

[271] Fraiser, *supra* note 269, at n.15 (2008) (citing State v. Anez, 108 Ohio Misc. 2d 18, 738 N.E.2d 491 (C.P. 2000)). For the majority approach, *see Horn*, 185 F. Supp. 2d at 561 (providing a chart of jurisdictions to accept failure of field sobriety tests as establishing probable cause for arrest or search).

B. The Case for a Heightened Standard for FRT

There is, however, a compelling justification for demanding a higher level of accuracy in FRT than in the cases of drug-sniffing dogs and sobriety tests: the Fourth Amendment allows drug-sniffs and sobriety tests only as incidents to already-lawful police stops.[272] In other words, one who has not been legitimately halted in his movement by the state cannot be subjected to either form of intrusion.[273] FRT surveillance, by contrast, subjects everyone's face to its algorithms' identification protocols.[274] Even if a state's FRT database is limited only to the photos of fugitives, the system must monitor all passersby without individualized suspicion.[275] Imagine, then, an FRT program with an error rate of even five percent, which would be considered excellent by canine or sobriety-test standards:[276] if the system is performing thousands of identifications per day,[277] then scores of blameless pedestrians will be searched or detained until their true identities are revealed.

Would the Fourth Amendment, which upholds "[t]he right of the people to be secure in their persons,"[278] tolerate such widespread error? In *Michigan Department of State Police v. Sitz*, the Court did allow the state to establish sobriety checkpoints that briefly tested each driver for intoxication.[279] The opinion held that the state's interest in decreasing highway deaths outweighed the momentary inconvenience to individuals of being stopped and tested.[280] Because the police encounters in *Sitz* were suspicionless and risked false positives, the government can point to the case as authorizing blanket FRT monitoring.[281] Yet the result in *Sitz* was motivated by the alarming "magnitude of the drunken driving problem," which the Court found responsible for "an annual death toll of

---

[272] The majority in *Illinois v. Caballes*, the Supreme Court case that ruled a dog-sniff is not a search, acknowledged that police may only use a drug-sniffing dog as an incident to a lawful stop. *Caballes*, 543 U.S. at 410. The majority in *Mich. Dep't of State Police v. Sitz* tolerated sobriety checks at a police roadblock only after finding that the stopping of the vehicles was itself justified. *Sitz*, 496 U.S. at 448–49.

[273] *See* James B. Johnston, *Drugs, Dogs, and the Fourth Amendment: An Analysis of Justice Stevens' Opinion in* Illinois v. Caballes, 24 QUINNIPIAC L. REV. 659, 676 (2006) (noting that *Caballes* requires inquiry into whether the traffic stop commenced and proceeded lawfully); *Edmond*, 531 U.S. at 47 (cautioning that sobriety testing is lawful only if it follows the example of *Sitz* or is motivated by individualized suspicion).

[274] *See supra* notes 27–33 and accompanying text.

[275] *See* PHILLIPS ET AL, *supra* note 9, at 6.

[276] *See* United States v. Diaz, 25 F.3d 392, 396 (6th Cir. 1994); State v. Superior Court, 149 Ariz. 269, app. A (Az. 1986).

[277] This is referred to as "large-population face recognition" or "LPFR" in NALINI KANTA RATHA & VENUGOPAL GOVINDARAJU, ADVANCES IN BIOMETRICS: SENSORS, ALGORITHMS AND SYSTEMS 363 (2008).

[278] U.S. CONST. amend. IV. Jed Rubenfeld has argued that the right protected in the Fourth Amendment is not a right to privacy *per se* but a "right of security," preventing the police from searching every house in a neighborhood where a fugitive has fled. Rubenfeld, *supra* note 76, at 119–25.

[279] *Sitz*, 496 U.S. at 455.

[280] *Id.* at 450–52.

[281] For examples of government briefs arguing to extend *Sitz* to new surveillance contexts, see Reply Brief for the Petitioner at 1-12, Illinois v. Lidster, 540 U.S. 419 (2004) (No. 02-1060) (information-gathering roadblock in response to single incident); Brief for Americans for Effective Law Enforcement, Inc. et al. as Amici Curiae in Support of the Petitioner at 5-10, Penn. Bd. of Probation and Parole v. Scott, 524 U.S. 357 (1998) (No. 97-581) (suspicionless searches of probationers' homes); Brief for Petitioners at 7-9, City of Indianapolis v. Palmer, 531 U.S. 32 (2000) (No. 99-1030) (roadblock for detecting drug use).

over 25,000" Americans.[282] Until face-based surveillance can be shown to combat a public harm of comparable magnitude, the probable cause standard should not allow error-prone technology to turn every civilian's outing into a potential police encounter.[283]

Perhaps, in the probable-cause context, the police tool by which courts should judge FRT is fingerprint analysis. Based on data from 2002, about 78% of American males and 54% of American females have been fingerprinted at some point in their lives,[284] and over the past two decades state and federal agencies have largely digitized their fingerprint archives.[285] As a result, a police search of an unidentified print likely filters through the fingerprints of millions of innocent civilians before finding a match.[286] This process is analogous to an FRT algorithm's identification phase, which filters an untagged set of facial dimensions through millions of pre-identified files.[287] Because the estimated failure rate of digital fingerprint-recognition software is low (about 2%),[288] society is not beset by false detentions stemming from algorithm error.[289] Only when the same can be said of FRT should its society-wide use survive probable-cause scrutiny.

VI. CONCLUSION

As innovations in digital surveillance have accelerated, fundamental uncertainties have emerged in Fourth Amendment jurisprudence. The fault lines of contemporary search-and-seizure law expose such questions as: whether we enjoy a reasonable expectation of anonymity in public, whether a person can be virtually "seized" by sophisticated technology that does not impede movement, and whether people truly cede privacy expectations in data revealed to ISPs. Face-recognition surveillance necessarily confronts each of these questions head-on, and, as a result, a constitutional challenge to

---

[282] *Sitz*, 496 U.S. at 451. In *City of Indianapolis v. Edmond*, the Court distinguished the checkpoint in *Sitz* from a police roadblock designed to detect a wider range of criminal wrongdoing. *Edmond*, 531 U.S. at 37–39.

[283] Sudden orders from authority, seemingly at random, to produce identification are evocative of the "roving patrols" that the Court has forcefully rebuked. *Almeida-Sanchez*, 413 U.S. at 274 ("Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government") (citing *Brinegar*, 338 U.S. at 180 (Jackson, J., dissenting)) (internal quotation marks omitted); *Ortiz*, 422 U.S. at 894, 910 (emphasizing that roving patrols are intended to "surprise" and often "frighten" unsuspecting motorists).

[284] ORC Intl., *Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector* 32 (2002), *available at* http://www.search.org/files/pdf/Biometricsurveyfindings.pdf.

[285] *See* Andrea Adelson, *Technology: Faster, More Accurate Fingerprint Matching*, N.Y. TIMES, Oct. 11, 1992, § 3, at 9; Gary Fields, *FBI Digitizes Fingerprint System Today*, USA TODAY, Aug. 10, 1999, at 1A; Hiawatha Bray, *Latest in High Tech Helps Police Keep Ahead of Criminals*, THE BOSTON GLOBE, July 10, 2006, at D1.

[286] Michael Cherry & Edward Imwinkelried, *How Can We Improve the Reliability of Fingerprint Identification*, 31 CHAMPION 36, 37–38 (2007) (describing functionality of the FBI's Automated Fingerprint Information System).

[287] *See supra* notes 2–7 and accompanying text.

[288] Michael Cherry & Edward Imwinkelried, *Forensics: A Cautionary Note About Fingerprint Analysis and Reliance on Digital Technology*, 30 CHAMPION 27, 28 (2006).

[289] For a comprehensive list of the known cases where the wrong person was arrested because of mistaken fingerprint identification, see Simon A. Cole, *More Than Zero: Accounting for Error in Latent Fingerprint Detection*, 95 J. CRIM. L. & CRIMINOLOGY 985, 1001–16 (2005).

this new technique may serve as a harbinger for the Fourth Amendment's ambit in the digital era. Courts will use the opportunity either to shore up the "right of the people to be secure," or to admit how little the Amendment safeguards once we emerge from our homes.