ANONYMITY, OBSCURITY, AND TECHNOLOGY: RECONSIDERING PRIVACY IN THE AGE OF BIOMETRICS

JONATHAN TURLEY[*]

ABSTRACT

For decades, cinematic and literary works have explored worlds without privacy: fishbowl societies with continual, omnipresent surveillance. For those worried about a post-privacy world, facial recognition technology and other biometric technology could well be the expanding portal to that dystopia. These technologies are rapidly transforming a society predicated on privacy into a diaphanous society where identity and transparency are defining elements. Biometric technology is perfectly suited to evade current privacy protections and doctrines because it presents new challenges to the existing legal framework protecting privacy. The greatest threat of this technological shift is to democratic activities—the very reason that countries such as China have invested so heavily into biometric surveillance systems.

This Article explores how our traditional privacy notions fit into a new age of biometrics. It seeks to frame the debate on what values society's notions of privacy protect, and how to protect them. After exploring prior approaches and definitions to privacy, it proposes a shift from an emphasis on anonymity to a focus on obscurity. The truth is that we now live in a "nonymous" world where our movements and associations will be made increasingly transparent. This Article concludes by recommending a comprehensive approach to biometric technology that would obscure increasingly available images and data while recasting privacy protections to fit a new and unfolding biometric reality. This obscurity will allow participation in society to continue unimpeded by the chilling effects created by the new technology. Without it, our democratic society will never be the same.

[*] J.B. and Maurice C. Shapiro Professor of Public Interest Law, The George Washington University Law School. I wish to thank The George Washington University Law School for the grants supporting the underlying research for this Article. I want to thank the participants of past hearings and conferences where this research was presented including the Presidential Commission on Law Enforcement and the Administration of Justice (July 2020), the CogX Conference of the United Kingdom's Centre for Data Ethics and Innovation (CDEI) (June 2020), and the AFCEA International Federal Identity Forum (Sept. 2019). I would also like to thank Tovah LaDier, James Loudermilk, and the other experts in this industry who generously offered insights on this Article. I also want to thank Nicholas Contarino for his research assistance.

CONTENTS

"There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. . . . You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."

—George Orwell, *1984*[1]

INTRODUCTION

From *1984*[2] and *Fahrenheit 451*[3] to *The Minority Report*[4] and *Total Recall*,[5] dystopian futures all have a common feature: continual, omnipresent surveillance of every citizen. The phobia of living in a fishbowl society is a shared phobia of all free people. It is also a growing reality for those living with increasingly less freedom in nations such as China. The technology that was merely a fiction when George Orwell penned *1984* now exists to make his dystopian vision a reality. That technology—and thus that future—has arrived with recent breakthroughs in biometric technology, including facial recognition technology ("FRT"). For many people, the popular release of an FRT function in Apple's iPhone was their first use of a biometric program, and it brought the same thrilling experience as the first encounter with the telephone or television. People are now accustomed to hearing businesses announce that voice recognition will be used during telephone calls with customers.

Automatic entries based on facial recognition are being explored at airports, movie theaters, and other businesses. In August 2019, Google announced that its 1.7 billion Android users would soon be using biometric identity authentication.[6] The move reflects a view that biometrics can reduce identity theft and password violations, an effort led in part by the industry group Fast

[1] GEORGE ORWELL, 1984, at 6-7 (Plume 1983) (1949).

[2] *Id.*

[3] RAY BRADBURY, FAHRENHEIT 451, at 138 (1953) ("'Police suggest entire population in the Elm Terrace area do as follows: Everyone in every house in every street open a front or rear door or look from the windows. The fugitive cannot escape if everyone in the next minute looks from his house. Ready!' Of course! Why hadn't they done it before! Why, in all the years, hadn't this game been tried! Everyone up, everyone out! He couldn't be missed!").

[4] MINORITY REPORT (Twentieth Century Fox & Dreamworks Pictures 2002). Walking through a mall, Chief John Anderton, played by actor Tom Cruise, has his eyes scanned by advertisements in order to target his interests. Later in the movie, Anderton's eyes are surgically replaced in order to avoid detection from police drones and their retinal scanners.

[5] TOTAL RECALL (Carolco Pictures 1990). Prior to taking a space bridge to the planet Mars, Douglas Quaid, played by actor Arnold Schwarzenegger, proceeds through a full body X-ray scanning machine to detect contraband.

[6] Davey Winder, *Google Confirms Password Replacement for 1.7 Billion Android Users*, FORBES (Aug. 13, 2019, 1:09 AM), https://www.forbes.com/sites/daveywinder/2019/08/13/google-confirms-password-replacement-for-17-billion-android-users-starting-now/#660291221000 [https://perma.cc/A9PH-QSD5].

Identity Online ("FIDO").[7] There are other positive uses of biometrics, including home security,[8] biometric guns that only work with a designated owner,[9] and biometric pet identification.[10] By 2023 biometrics are expected to authenticate $2 trillion in commercial transactions.[11] These "frictionless" transactions include the rising use of biometric wallets that are replacing credit cards around the world.[12] The new technology is viewed as liberating for a market hampered by security threats. Just as government surveillance can have a chilling effect on speech and associations, the vulnerability of online transactions and files to

[7] FIDO seeks to incorporate logins with biometric security. *FIDO Certification Programs: Introducing New Biometric Component Certification, Authenticator Levels and Certified Companies*, FIDO ALLIANCE (Sept. 6, 2018), https://fidoalliance.org/fido-certification-programs-introducing-new-biometric-component-certification-authenticator-levels-and-certified-companies/ [https://perma.cc/7GHD-MU3E].

[8] *See* Apri Siswanto, Norliza Katuk & Ku Ruhana Ku-Mahamud, *Biometric Fingerprint Architecture for Home Security System*, 3 INNOVATION & ANALYTICS CONF. & EXHIBITION 137, 138-41 (2016).

[9] Biometric or "smart" guns could radically reduce the incidence of child shootings in homes. *See* Ashley Luthern, Ryan J. Foley & Nick Penzenstadler, *Nationally, Children Die in Accidental Shootings at Pace of One Every Other Day*, MILWAUKEE J. SENTINEL (Oct. 16, 2016, 10:42 PM), https://www.jsonline.com/story/news/crime/2016/10/14/nationally-children-die-accidental-shootings-pace-one-every-other-day/92013540/ [https://perma.cc/BCN8-TLEA]. During his campaign, President-Elect Biden raised the use of biometric guns as a possible national reform. Makena Kelly, *Biden Pushes Smart Guns as Solution for Gun Violence During Primary Debate*, VERGE (June 27, 2019, 11:01 PM), https://www.theverge.com/2019/6/27/18952042/joe-biden-smart-gun-control-democratic-debate-2020-regulation-biometric-trigger. Notably, gun companies have received some resistance from existing gun owners on this use of biometric technology. Nicole Nguyen, *Here's What's Up with "Smart Guns" – and Why You Can't Buy One in the US*, BUZZFEED NEWS (Mar. 13, 2018, 5:02 PM), https://www.buzzfeednews.com/article /nicolenguyen/what-is-smart-gun-technology [https://perma.cc/SK6S-NTHF] ("After Colt and Smith & Wesson, two major US gun manufacturers, agreed in 2000 to create government-sponsored smart guns to prevent accidental shootings and gun deaths, a boycott from gun owners nearly drove them out of business." (citations omitted)).

[10] China has a technology that is based on the fact that dog noses are unique. Natt Garun, *A Chinese AI Startup Is Tracking Lost Dogs Using Their Nose Prints*, VERGE (July 13, 2019, 2:00 PM), https://www.theverge.com/2019/7/13/20693064/megvii-chinese-ai-facial-recognition-lost-pets-dogs-cats-surveillance.

[11] Press Release, Juniper Res., Mobile Biometrics to Authenticate $2 Trillion of Sales by 2023, Driven by Over 2,500% Growth (July 24, 2018), https://www.juniperresearch.com /press/press-releases/mobile-biometrics-to-authenticate-2-tn-sales-2023 [https://perma.cc/VU9N-3R9Z].

[12] Quentin Fottrell, *Silicon Valley's Final Frontier for Payments: 'The Neoliberal Takeover of the Human Body,'* MARKETWATCH (Oct. 23, 2019, 12:59 PM), https://www.marketwatch.com/story/the-technology-that-should-finally-make-your-wallet-obsolete-2019-09-06 [https://perma.cc/3HWB-MJK6].

hacking and theft has been found to have a chilling effect on its use.[13] Perceived security provided by biometric technology could largely eliminate that effect.

The added security and convenience of biometric technology, including new devices allowing homeowners to face scan visitors, have resonated with the public.[14] In a curious way, biometric technology—and FRT in particular—can even appeal to an innate vanity in using a technology that will accept only you as you. In a celebrity-driven world, these products give everyone a sense of digital celebrity status. Google programs show you an ever-expanding range of people connected to your social media activities—making everyone a Kevin Bacon with digital degrees of separation from an ever-expanding group of people.[15] One Chinese program enables people to insert themselves as stars into movies by allowing their face prints to be copied and stored in a databank.[16] Retailers are already incorporating FRT to identify VIP customers.[17] One company, CLEAR, has run national commercials featuring a person named Jimmy who is able to gain unique satisfaction from the convenience of immediate recognition by FRT at an airport.[18] The narrator proudly proclaims that Jimmy will no longer have to stand in line "just to prove he's really Jimmy."[19] Of course, the liberation that Jimmy feels in his first encounter with FRT poses a more sinister prospect for civil libertarians. For all of its security

[13] In 2016, the Commerce Department's National Communications and Information Administration completed a study showing that "[f]orty-five percent of online households reported that [privacy and security] concerns stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet, and 30 percent refrained from at least two of these activities." Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOMM. & INFO. ADMIN.: BLOG (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities [https://perma.cc/9F9K-ERV3].

[14] Molly Price, *Smart Home Cameras Bring Facial Recognition Ethics to Your Front Door*, CNET (Apr. 2, 2019, 5:00 AM), https://www.cnet.com/news/smart-home-cameras-bring-the-facial-recognition-ethical-dilemma-to-your-front-door/ [https://perma.cc/73G6-32E9].

[15] Ironically, the actor himself said that he was "horrified" to see how everyone in Hollywood seemed only six degrees of separation from his movies. Brandon Griggs, *Kevin Bacon on 'Six Degrees' Game: 'I Was Horrified,'* CNN BUS. (Mar. 12, 2014, 8:13 AM), https://www.cnn.com/2014/03/08/tech/web/kevin-bacon-six-degrees-sxsw/index.html [https://perma.cc/7NUW-CXA5].

[16] Shan Li, *Deepfake Chinese App Zao Faces Privacy Backlash; 'I'm Scared,'* WALL STREET J., Sept. 4, 2019, at A8.

[17] Brenda Salinas, *High-End Stores Use Facial Recognition Tools to Spot VIPs*, NPR (July 21, 2013, 6:21 AM), https://www.npr.org/sections/alltechconsidered/2013/07/21/203273764/high-end-stores-use-facial-recognition-tools-to-spot-vips [https://perma.cc/FT77-NJK4].

[18] *CLEAR TV Commercial, 'Jimmy,'* ISPOT.TV, https://www.ispot.tv/ad/dWRZ/clear-jimmy (last visited Nov. 18, 2020).

[19] *Id.*

and commercial advantages, this transformative technology presents chilling threats for free speech, privacy, and associational rights.

Most countries are currently investing in some form of biometric technology, particularly at airports and border entry points. China, Russia, and the United States have been the most prominent investors in this technology. The result is a market that is expected to exceed $7 billion a year by 2022.[20] Some estimates predict an increase in market share for FRT alone as high as $10.9 billion by 2025.[21] Given that the estimate for this market was $3.85 billion in 2017, these projections exemplify the impressive growth that FRT is expected to have in the near future.[22]

The extensive use of FRT in both commercial and security applications is already on display in many countries, especially in China. Shanghai Hongqiao International Airport has already deployed self-service kiosks for flight and baggage check-in.[23] Passengers will be cleared through security clearance and boarding with FRT programs that confirm their identities within seconds.[24] Even some vending machines now operate using FRT.[25]

---

[20] *Facial Recognition Market 2017 by Component, Technology, Use Case, End-User, and Region*, BUS. WIRE (Dec. 1, 2017, 9:30 AM), https://www.businesswire.com/news/home/20171201005396/en/ [https://perma.cc/29H3-SY97]. A report issued by Markets and Markets in June 2019 projected that facial recognition market size could grow from $3.2 billion in 2019 to $7.0 billion in 2024, at a compound annual growth rate of 16.6%. *Facial Recognition Market Worth $7.0 Billion by 2024*, MKTS. & MKTS. (June 27, 2019), https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp [https://perma.cc/NQH9-3RLZ].

[21] *Facial Recognition Market - Growth, Trends, and Forecasts (2020 - 2025)*, MORDOR INTELLIGENCE, https://www.mordorintelligence.com/industry-reports/facial-recognition-market [https://perma.cc/HU2C-WZAY] (last visited Nov. 18, 2020). Grand View Research in March 2020 valued the facial recognition market size at $3.4 billion in 2019 and projected that it would expand at a compound annual growth rate of 14.5% from 2020 to 2027, with a worth approximately $10 billion in 2027. *Facial Recognition Market Size, Industry Report, 2020-2027*, GRAND VIEW RES. (Mar. 2020), https://www.grandviewresearch.com/industry-analysis/facial-recognition-market [https://perma.cc/EK9Q-FUQZ].

[22] *Global Facial Recognition Market Report 2018*, PR NEWSWIRE (June 5, 2018, 5:00 AM), https://www.prnewswire.com/news-releases/global-facial-recognition-market-report-2018-300660163.html [https://perma.cc/C962-4PF4]. On June 8, 2020, PR Newswire reported that the FRT market size was projected to grow from $3.54 billion in 2019 to $9.99 billion in 2025, at a compound annual growth rate of 18.84%. *Facial Recognition Market Size to Reach USD 9.99 Billion by 2025*, PR NEWSWIRE (June 8, 2020, 8:14 PM), https://www.prnewswire.com/news-releases/facial-recognition-market-size-to-reach-usd-9-99-billion-by-2025--valuates-reports-301071952.html [https://perma.cc/C5PK-D9FM].

[23] Erika Kinetz, *Shanghai Airport Automates Check-In with Facial Recognition*, SEATTLE TIMES (Oct. 17, 2018, 1:01 PM), https://www.seattletimes.com/business/check-in-with-facial-recognition-now-possible-in-shanghai/ [https://perma.cc/8GWB-RVG3].

[24] *Id.*

[25] Isobel Asher Hamilton, *A Futuristic Chinese TikTok Video Shows a Woman Paying for Vending Machine Items with No Money or Card — Just Her Face*, BUS. INSIDER (Aug. 22,

China's investment, however, has an even greater political design. The Chinese government has openly tried to create the very fishbowl society abhorred in dystopian novels and movies. The behavioral impact of FRT has long been a draw for authoritarian countries for obvious reasons. Individuals will be reluctant to attend protests or meetings if government can ascertain their identity. They are also unlikely to associate with individuals or businesses that are deemed problematic by the government, particularly when the Chinese government is expanding its "citizen score" system by tying travel and other privileges to an individual's conduct.[26] Notably, the greatest concern voiced by protesters in the 2019 protests in Hong Kong was evading FRT systems.[27] Not surprisingly, much of the FRT efforts in China have been directed at minority communities, including Uighurs and other populations viewed as a threat to the authoritarian regime.[28] With the world's largest network of cameras in public spaces, China incorporated FRT to create a fearsome surveillance system. In one month alone, officials in the city of Sanmenxia screened 500,000 images of Uighur people.[29] Police called it "minority identification," a system that has been denounced for its ability to categorize and identify people based on their ethnicity.[30] Indeed, Chinese companies are now selling programs with a "minority recognition function."[31] China is currently completing the largest FRT system in the world—aimed at identifying any one of its 1.3 billion citizens within three seconds with a 90% accuracy rate.[32] Once completed, the already

2019, 8:48 AM), https://www.businessinsider.com/a-tiktok-from-china-shows-facial-recognition-equipped-vending-machine-2019-8 [https://perma.cc/X6EP-ADPQ].

[26] Charlie Campbell, *How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens*, TIME, https://time.com/collection/davos-2019/5502592/china-social-credit-score/ [https://perma.cc/LVM8-5EL9] (last visited Nov. 18, 2020).

[27] Paul Mozur, *Streets Clogged by the Faceless*, N.Y. TIMES, July 27, 2019, at A1.

[28] Paul Mozur, *Facial Scans Tighten China's Grip on a Minority*, N.Y. TIMES, Apr. 15, 2019, at A1 ("The facial recognition technology, which is integrated into China's rapidly expanding networks of surveillance cameras, looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review.").

[29] *Id.* at A8.

[30] *Id.* Other governments have been challenged over the use of FRT against persecuted minority populations. In Brazil's famous Copacabana neighborhood, the government installed traffic and security cameras onto poles and buildings ahead of the Carnival. Melissa Locker, *Brazil Is Using a Facial Recognition System During Rio's Carnival*, FAST CO. (Jan. 30, 2019), https://www.fastcompany.com/90299268/brazil-is-using-facial-recognition-tech-during-rios-carnival [https://perma.cc/GP6W-J6TV]. Although ostensibly this move was made to prevent crime, it raised eyebrows given the government's anti-LGBTQ agenda and the Carnival's traditionally inclusive nature. *Id.*

[31] Mozur, *supra* note 28, at A8.

[32] *See* Stephen Chen, *China to Build Giant Facial Recognition Database to Identify Any Citizen Within Seconds*, S. CHINA MORNING POST (Oct. 12, 2017, 9:00 PM), https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any [https://perma.cc/24LS-N79L].

limited ability of citizens in China to engage in protests or reform activities will be sharply reduced. China's interest in FRT is not only political; it is also economic. China and Russia are quickly dominating this expanding international market. YITU Technology in Shanghai, China, and other Chinese companies have produced seven of the ten highest performing algorithms in the world;[33] Microsoft is also believed to be using a Chinese algorithm.[34]

Russia also seems eager to deploy FRT and is combining its own algorithms with its massive public surveillance system.[35] In January 2020, Moscow deployed a new "live" facial recognition system throughout the city.[36] In Moscow alone, there are more than 160,000 cameras that will now sweep the streets with FRT to identify individuals and track their movements.[37] A Russian company, Moscow-based NtechLab, even won the first FRT competition held by the U.S. National Institute of Standards and Technology ("NIST") in 2017.[38]

---

[33] B. Scott Swann & James Loudermilk, *Facial Recognition: A Strategic Imperative for National Security*, BIOMETRIC UPDATE (June 3, 2019), https://www.biometricupdate.com/201906/facial-recognition-a-strategic-imperative-for-national-security [https://perma.cc/UN2D-A4VS] ("In a growing trend, algorithms from YITU Technology in Shanghai, China have turned in top performances in [U.S. National Institute of Standards and Technology's one-to-one] match tests in recent years."). Notably, recent reports show how competitive this market has become because of emerging new products and algorithms. The tenth ranked performer came from a Lithuanian company. Yet, in the September 11, 2019 report from the U.S. National Institute of Standards and Technology ("NIST") for verification (using one-to-one image comparisons), it determined that only three of the top ten are Chinese algorithms: two are Russian, two are American, two are British, and one is Slovakian. PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 41-44 (2019) [hereinafter NIST 2019 TEST], https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf [https://perma.cc/NE3N-3FSS].

[34] Swann & Loudermilk, *supra* note 33.

[35] *Large-Scale Facial Recognition Coming to Russian Airports in 18 Months*, ETURBONEWS (Aug. 27, 2019, 11:18 PM), https://www.eturbonews.com/263257/large-scale-facial-recognition-coming-to-russian-airports-in-18-months/ [https://perma.cc/N9UF-S3H8].

[36] James Vincent, *Moscow Rolls Out Live Facial Recognition System with an App to Alert Police*, VERGE (Jan. 30, 2020, 11:13 AM), https://www.theverge.com/2020/1/30/21115119/moscow-live-facial-recognition-roll-out-ntechlab-deployment. Russia is already using FRT during the COVID-19 pandemic to track potential carriers who have violated their quarantine. Kaelan Deese, *Russia Using Facial Recognition Technology to Track Coronavirus Quarantine*, HILL (Feb. 21, 2020), http://thehill.com/policy/technology/technology/484048-russia-using-facial-recognition-technology-to-track-coronavirus [https://perma.cc/K5X6-PTAQ].

[37] Matt Hamblen, *Moscow's Smart Tech Includes 160,000 Outdoor Cameras*, COMPUTERWORLD (Feb. 28, 2017, 9:46 AM), https://www.computerworld.com/article/3175063/moscows-smart-tech-includes-160000-cameras-to-detect-traffic-violators.html [https://perma.cc/Z4RZ-LHNT].

[38] PATRICK GROTHER & MEI NGAN, NAT'L INST. OF STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST PART 1: VERIFICATION 3 (2017); *see also* Kenneth Rapoza, *Russia*

That company developed FindFace Security, which Russia claims that it used to identify 180 wanted criminals during the 2018 Summer World Cup.[39] The FindFace smartphone app allows people to take a person's photo and then find their social media accounts.[40] NtechLab is currently issuing portable video recorders and glasses with FRT capabilities.[41] This work is being done in conjunction with Chinese companies, including Dahua Technology, which appeared on a list for banning in the United States beginning in August 2019.[42] On the commercial side, a Russian company issued a program that could be used to perform facial recognition on the Russian social media site VKontakte. The program, searchface.ru, even allowed users to open locked accounts, which led to lawsuits in 2019.[43] Other commercial products include FRT programs that recognize and report tired taxi drivers who remain under constant surveillance.[44]

The United States has also made significant investments in FRT. In 2017, the government used FRT at nine airports for its Biometric Entry-Exit Program.[45]

No. 1 in Facial Recognition, According to Official Washington Spycraft Techies, FORBES (Nov. 28, 2017, 12:42 PM), https://www.forbes.com/sites/kenrapoza/2017/11/28/russia-no-1-in-facial-recognition-according-to-official-washington-spycraft-techies/#3d2c9576fc70 [https://perma.cc/8AYJ-NKT3].

[39] Victoria Zavyalova, *In Your Face: New Facial Recognition System Catches Criminals in Russia*, RUSS. BEYOND (Nov. 27, 2018), https://www.rbth.com/science-and-tech/329587-facial-recognition-system-catches-criminals [https://perma.cc/8LPA-MJGV].

[40] Darlene Storm, *Face Recognition App FindFace May Make You Want to Take Down All Your Online Photos*, COMPUTERWORLD (May 18, 2016, 9:46 AM), https://www.computerworld.com/article/3071920/face-recognition-app-findface-may-make-you-want-to-take-down-all-your-online-photos.html [https://perma.cc/A5R7-E4CC] ("FindFace facial recognition may not be brand new, but the app boasts of a 70% accuracy as in snap a photo of a stranger and then find out who that person is via their social media profile." (citation omitted)).

[41] Stephen Mayhew, *Moscow Police Piloting AR Glasses with NTechLab Facial Recognition Tech*, BIOMETRIC UPDATE (Feb. 24, 2019), https://www.biometricupdate.com/201902/moscow-police-piloting-ar-glasses-with-ntechlab-facial-recognition-tech [https://perma.cc/RSE8-GUDU].

[42] Vladimir Kozlov, *Russia Develops a Major Face-Recognition Scheme*, BNE INTELLINEWS (June 25, 2019), https://intellinews.com/russia-develops-a-major-face-recognition-scheme-162959/?source=russia [https://perma.cc/45KE-4WU2].

[43] *See* Chris Burt, *Site Using Facial Recognition to Match Photos from Russian Social Media Network Sued*, BIOMETRIC UPDATE (Feb. 18, 2019), https://www.biometricupdate.com/201902/site-using-facial-recognition-to-match-photos-from-russian-social-media-network-sued [https://perma.cc/3FH5-U2TA].

[44] Amrita Khalid, *Facial Recognition Will Catch Sleepy Taxi Drivers in Russia*, ENGADGET (Aug. 8, 2019), https://www.engadget.com/2019/08/08/facial-recognition-will-catch-sleepy-taxi-drivers-in-russia/ [https://perma.cc/RCX9-6BPL].

[45] Anthony Kimery, *Progress Made, but CBP Still Confronts Challenges Implementing Biometric Entry-Exit Program*, BIOMETRIC UPDATE (Sept. 26, 2018) https://www.biometricupdate.com/201809/progress-made-but-cbp-still-confronts-challenges-implementing-biometric-entry-exit-program [https://perma.cc/T7K8-4PU9].

Biometric e-Gates are currently operating at U.S. airports, including LAX in California, MIA and MCO in Florida, and JFK in New York.[46] The TSA is also testing programs at other airports including LAS in Nevada.[47] Customs and Border Protection ("CBP") claims that this pilot program was able to confirm passenger identities with exceptional speed and accuracy by logging photos for over 98% of passengers in internal databases.[48] Yet, due to both technical and operational problems, the actual match rate may be closer to 85%.[49] The current goal is to have the accuracy rate at 98% by 2021 for identification of all foreign departures.[50] This biometric system was not only funded as part of the Consolidated Appropriations Act of 2016 but also ordered to be implemented by Executive Order 13,780.[51]

In addition to the entry-exit program, various U.S. agencies already utilize biometric technology with a massive collection of data. The FBI is estimated to have access to 641 million facial images as part of its Facial Analysis, Comparison, and Evaluation ("FACE") program.[52] In 2016, roughly 30 million such images were claimed to be part of the FBI's Interstate Photo System of mugshots.[53] The rest were mined from databanks ranging from passport to

[46] Sean O'Kane, *British Airways Brings Its Biometric Identification Gates to Three More US Airports*, VERGE (Mar. 9, 2018, 12:17 PM), https://www.theverge.com/2018/3/9/17100314/british-airways-facial-recognition-boarding-airports.

[47] Brandi Vincent, *TSA Launches Facial Recognition Pilot at Las Vegas Airport*, NEXTGOV (Aug. 27, 2019), https://www.nextgov.com/emerging-tech/2019/08/tsa-launches-facial-recognition-pilot-las-vegas-airport/159479/ [https://perma.cc/U2G9-58ZV].

[48] DEP'T OF HOMELAND SEC. OFFICE OF INSPECTOR GEN., OIG-18-80, PROGRESS MADE, BUT CBP FACES CHALLENGES IMPLEMENTING A BIOMETRIC CAPABILITY TO TRACK AIR PASSENGER DEPARTURES NATIONWIDE 6 (2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf [https://perma.cc/587F-AGQJ]; Jack Corrigan, *U.S. Customs Wants to Use Your Face As a Boarding Pass*, NEXTGOV (Feb. 20, 2018), https://www.nextgov.com/emerging-tech/2018/02/us-customs-wants-use-your-face-boarding-pass/146115/ [https://perma.cc/RR3U-J7H8]. American Airlines has already rolled out its FRT system for passengers. Sinéad Baker, *American Airlines Has Launched Facial Recognition at the Boarding Gate, Part of a Trend Sweeping US Airports*, BUS. INSIDER (Aug. 29, 2019, 9:57 AM), https://www.businessinsider.com/american-airlines-facial-recognition-boarding-dfw-aviation-trend-2019-8 [https://perma.cc/L4NR-6LT2].

[49] DEP'T OF HOMELAND SEC. OFFICE OF INSPECTOR GEN., *supra* note 48, at 6.

[50] *Id.*

[51] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242, 2493; Exec. Order No. 13,780, 82 Fed. Reg. 13,209, 13,216 (Mar. 9, 2017).

[52] U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, FACE RECOGNITION TECHNOLOGY: DOJ AND FBI HAVE TAKEN SOME ACTIONS IN RESPONSE TO GAO RECOMMENDATIONS TO ENSURE PRIVACY AND ACCURACY, BUT ADDITIONAL WORK REMAINS (2019), https://www.gao.gov/assets/700/699489.pdf [https://perma.cc/DH2H-NHH2]. That is inclusive of state DMV photos under active memorandums of understanding, though it is not believed to have active search capabilities of all such state systems. *Id.* at 4 n.7.

[53] *Id.* at 16.

driver's license photos.[54] In 2014, the FBI's Next Generation Identification ("NGI"), moving ahead with little attention from Congress or the media, introduced a Rap Back Service which allows employers to share employees' biometric data with the FBI as part of background checks for licensing and employment in sensitive positions.[55] Likewise, the Department of Defense ("DoD") implemented a highly advanced Automated Biometric Identification System ("ABIS") that interacts with other databanks and can cross-check facial recognition, palm prints, fingerprints, irises, and other biometric data on individuals.[56] Special forces now have handheld devices that can scan a face in Afghanistan and receive virtually immediate identification and information on millions of individuals.[57] The domestic incorporation of this FRT extends to municipal law enforcement; for example, the New York Police Department is currently storing pictures of individuals as young as eleven years old.[58] The New York Education Department has also moved toward the use of FRT on students, though that effort was met with opposition.[59] FRT has divided Detroit with many proponents, including the Chief of Police, demanding its use to curtail the city's chronic crime problems.[60]

The use of FRT and other biometric technology by governments is only a small fraction of its use in the private industry, with dozens of companies in the

[54] *Id.* at 5.

[55] This information is exchanged in accordance with over 2000 statutes with such background check provisions under Public Law Number 92-544, 86 Stat. 1109, 1115 (1972). States can sign up for Rap Back as part of this system, though only Utah initially opted to do so. More states are expected to join in the coming years. UTAH CODE ANN. § 53-10-108(14) (West 2020); *see also* Pub. L. No. 92-544, 86 Stat. 1109, 1115 (1972); Ava Kofman, *The FBI Is Building a National Watchlist That Gives Companies Real-Time Updates on Employees*, INTERCEPT (Feb. 4, 2017, 9:19 AM), https://theintercept.com/2017/02/04/the-fbi-is-building-a-national-watchlist-that-gives-companies-real-time-updates-on-employees/ [https://perma.cc/STS9-3476] (explaining that while a majority of states had in-state Rap Back programs since 2007, states and agencies can now partner with federal government to enter data into FBI's NGI database).

[56] *Frequently Asked Questions*, DEF. FORENSICS & BIOMETRICS AGENCY, https://www.dfba.mil/about/faqs.html [https://perma.cc/Q2LT-FF29] (last visited Nov. 18, 2020) (listing assets maintained by Defense Forensics and Biometrics Agency for purposes of ABIS program).

[57] Thom Shanker, *To Track Militants, U.S. Has System that Never Forgets a Face*, N.Y. TIMES, July 14, 2011, at A1 (noting that soldiers and police officers take digital scans of eyes, faces, and fingerprints).

[58] Joseph Goldstein & Ali Watkins, *In New York, Police Computers Scan Faces, Some as Young as 11*, N.Y. TIMES, Aug. 2, 2019, at A1.

[59] *Id.* (explaining that state Education Department told the school district of Lockport, New York to delay plans to use facial recognition on students).

[60] Erin Einhorn, *A Fight Over Facial Recognition Is Dividing Detroit – with High Stakes for Police and Privacy*, NBC NEWS (Aug. 22, 2019, 4:44 AM), https://www.nbcnews.com/news/us-news/fight-over-facial-recognition-dividing-detroit-high-stakes-police-privacy-n1045046 [https://perma.cc/TR2V-B3S3].

United States alone producing products for private and law enforcement use.[61] The exponential growth of FRT applications and other biometric technology has led to some legislative proposals, but much of this industry remains largely unregulated.[62] Despite the lack of legislative restraints, private companies have faced pressure over the use of FRT. And companies like IBM, Amazon, and Microsoft have halted or scaled back on the production of FRT products for law enforcement uses.[63]

The pressure on these companies reflects growing questions over the use and accuracy of this technology, including the sharing of facial images by federal and state agencies. Immigration and Customs Enforcement ("ICE") agents' use of state driver's license records for FRT databanks is an example of the expanding usage of facial imagery.[64] The FBI's NGI project relies on the Interstate Photo System to run images from both private and public sources.[65] The storage of massive amounts of biometric data for government uses is expanding exponentially.[66] A recent security breach in China that exposed millions of facial-recognition files highlighted the prospect that facial imagery could be stolen and manipulated.[67]

The greatest controversies focus on the accuracy of biometric technology, specifically FRT. Various studies have shown a high rate of error, particularly

[61] For a list of sixteen industries that have been impacted by the introduction of FRT, see generally CB INSIGHTS, GAME-CHANGING TECH OR DYSTOPIAN NIGHTMARE? HOW 16 INDUSTRIES COULD BE TRANSFORMED BY FACIAL RECOGNITION (2019) (on file with the Boston University Law Review).

[62] The latest such legislative proposal is the National Biometric Information Privacy Act submitted by Senators Jeff Merkley and Bernie Sanders. National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2020) (proposing a bill "[t]o regulate the collection, retention, disclosure, and destruction of biometric information"). The law would require private companies and corporations to get written consent to collect biometric data. *Id.* § 3(b)(1)(B)(ii).

[63] Rebecca Heilweil, *Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress.*, VOX (June 11, 2020, 5:02 PM), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police. While IBM took a strong stance against FRT, noting the technology's potential for abuse or misuse, Amazon and Microsoft both took softer stances, suggesting that they remain open to the use of the technology in the future. *Id.*

[64] Catie Edmondson, *ICE Used Facial Recognition to Scan Driver Databases*, N.Y. TIMES, July 8, 2019, at A16.

[65] *Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi [https://perma.cc/4Z5E-CAL5] (last visited Nov. 18, 2020).

[66] *See id.* (noting that, as advancements in technology allowed for further development of biometric identification, NGI system necessarily adapted to meet "evolving business needs").

[67] Kate O'Flaherty, *Facial Recognition at U.S. Airports. Should You Be Concerned?*, FORBES (Mar. 11, 2019, 2:01 PM), https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/facial-recognition-to-be-deployed-at-top-20-us-airports-should-you-be-concerned/#6be3c5c37d48 [https://perma.cc/529C-37G3].

with racially and ethnically diverse people.[68] Also still struggling with false identifications among particular racial and ethnic groups, top FRT products continue to perform at very high accuracy rates overall.[69] NIST found "empirical evidence" that many facial recognition algorithms showed "demographic differentials" due to a person's age, gender, or race.[70] These controversies have resulted in calls to ban FRT in various states.[71] Due to the tremendous demand and development of the private FRT industry it is doubtful that these measures will successfully bar the use of biometric technology. However, this legitimate concern over accuracy magnifies the existing concerns over privacy in the rapid expansion of this technology.

Juxtaposed to this growing technological threat is a body of privacy case law that rest largely on the same foundation initially described in Samuel Warren and Louis Brandeis's celebrated 1890 work, "The Right to Privacy."[72] Warren and Brandeis articulated an emerging right in a transforming society: "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."[73] Beginning with privacy interests in property and physical spaces, privacy has

[68] *See, e.g.*, K.S. Krishnapriya, Kushal Vangara, Michael C. King, Vítor Albiero & Kevin Bowyer, *Characterizing the Variability in Face Recognition Accuracy Relative to Race*, 2019 IEEE CONF. ON COMPUTER VISION & PATTERN RECOGNITION WORKSHOPS 2278 (investigating differences in facial recognition accuracy between Black and Caucasian images and finding that the Black group had higher false match rate and lower false nonmatch rate); Inioluwa Deborah Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, 2019 CONF. ON ARTIFICIAL INTELLIGENCE ETHICS & SOC'Y 429, 429, 434 (conducting "algorithmic audit of gender and skin type performance disparities in commercial facial analysis models" and concluding that "significant subgroup performance disparities persist"); *see also* Cynthia M. Cook, John J. Howard, Yevgeniy B. Sirotin, Jerry L. Tipton & Arun R. Vemury, *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, 1 IEEE TRANSACTIONS ON BIOMETRICS BEHAV. & IDENTITY SCI. 32 (2019) (examining effect of demographic factors on performance of eleven commercial face biometric systems tests and finding that darker skin reflectance gave rise to less accurate readings).

[69] Raji & Buolamwini, *supra* note 68, at 434.

[70] Drew Harwell, *Federal Study Finds Racial Bias in Facial-Recognition Systems*, WASH. POST, Dec. 20, 2019, at A22.

[71] *See, e.g.*, Letter from Marc Rotenberg, President, Elec. Privacy Info. Ctr.; Caitriona Fitzgerald, Policy Dir., Elec. Privacy Info. Ctr. & Jeramie Scott, Senior Counsel, Elec. Privacy Info. Ctr., to James B. Eldridge, Chair, Joint Comm. on the Judiciary, Gen. Court of the Commonwealth of Mass. & Claire D. Cronin, Chair, Joint Comm. on the Judiciary, Gen. Court of the Commonwealth of Mass. (Oct. 22, 2019), https://epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf [https://perma.cc/K7C4-YMFL].

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

[73] *Id.* at 193.

expanded to include protections over procreational choices[74] and other areas related to personal autonomy.[75] Yet, these expansions were incremental, particularly the evolution of the conceptual basis for privacy interests. Writers like Roscoe Pound,[76] Louis Henkin,[77] and Paul Freund[78] have tied privacy to concepts of personhood or autonomy, but the linkage of privacy to personality has not penetrated far into actual legal decisions.

The rise of FRT and biometric technology places great stress on that very linkage. That technology implicates the loss of freedom to move and interact in public spaces without fear of being recognized or tracked. That loss impacts the ability of individuals to freely form new experiences, associations, and viewpoints. Indeed, some FRT developers and investors have dismissed privacy as a dated concept outstripped by technology. David Scalzo, an investor with Kirenaga Partners, was quoted in 2020 as saying, "I've come to the conclusion that because information constantly increases, there's never going to be privacy . . . . Laws have to determine what's legal, but you can't ban technology. Sure, that might lead to a dystopian future or something, but you can't ban it."[79] We actually can ban it. The question is whether technology and privacy is truly now a zero-sum game.

Courts' decisions on FRT and biometric technology remain sparse, but the U.S. Court of Appeals for the Ninth Circuit, in *Patel v. Facebook, Inc.*,[80] recently ruled against Facebook, which was challenging a class action based on the nonconsensual collection of users' face prints.[81] The court found that such nonconsensual collection was a cognizable injury and allowed the application of the Illinois Biometric Information Privacy Act ("BIPA") as a cause of action for conduct occurring outside of the state.[82] In 2010, Facebook released "Tag

[74] *See* Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965) (holding unconstitutional Connecticut statute banning use of contraceptives).

[75] The Court has declared that "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education" are key to personal autonomy. Whalen v. Roe, 429 U.S. 589, 600 n.26 (1977) (quoting Paul v. Davis, 424 U.S. 693, 713 (1976)). The Court further stated, "[C]ases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions." *Id.* at 598-600 (footnotes omitted).

[76] Roscoe Pound, *Interests of Personality*, 28 HARV. L. REV. 445, 445, 451, 453 (1915).

[77] Louis Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1424-25 (1974).

[78] Paul A. Freund, *Friday Evening Session – Annual Dinner*, 52 A.L.I. PROC. 568, 574-75 (1975).

[79] Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. TIMES, Feb. 10, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[80] 932 F.3d 1264 (9th Cir. 2019).

[81] *Id.* at 1271.

[82] *Id.* at 1273 (concluding that developing face template using FRT without consent "invades an individual's private affairs and concrete interests"); *see also* 740 ILL. COMP. STAT.

Suggestions," a program that allows FRT to identify friends in photos uploaded by the user.[83] The program makes a face print of people in the photos and "tags" individuals identified in the photo.[84] This produces a massive data bank of face prints that are held in six different data centers located around the United States. The court found that FRT represented the latest and possibly most significant challenge of new technology to privacy interests.

> Taking into account the future development of such technology as suggested in [*Carpenter v. United States*, 138 S. Ct. 2206, 2216 (2018)], it seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cell phone. We conclude that the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests.[85]

While *Patel* focused on the criteria for a class action and proper jurisdiction, it is a stark recognition of the emerging threat that biometric technology poses to traditional privacy. The use of a state law, however, to effectively establish a new biometric privacy standard is unworkable and threatens a patchwork of different approaches to the technology. At the same time, as discussed below, Europe has been reworking its own privacy standard to address this new technology.[86] The rapid expansion of biometric products has far outstripped the courts' ability to address the legal issues raised by the technology.

The result is not only inimical to privacy values but also to other interests that are impacted by these programs. For example, a recent New York ruling addressed a request for the filming of proceedings in state court. Such requests raise important interests of the free press as well as public access to judicial proceedings. However, the court refused the request in *C.C. v. D.D.*,[87] in part due to the ability of FRT to identify people in the courtroom.[88] The court noted that, "[p]resumably, there are other facial recognition platforms, not only Facebook, any of which could, either now or in the future, identify these parties

14/20 (2020) (providing that "[a]ny person aggrieved by a violation" of the statute's provisions "shall have a right of action . . . against an offending party").

[83] *Patel*, 932 F.3d at 1268.

[84] *Id.*

[85] *Id.* at 1273.

[86] Mehreen Khan, *EU Plans Crackdown on Use of Facial Recognition in Public Areas*, FIN. TIMES, Aug. 23, 2019, at 1 ("The European Commission is planning regulation that will give EU citizens rights over the use of their of facial recognition data as part of an overhaul in the way Europe regulates artificial intelligence . . . ."); *see also infra* note 480 and accompanying text (discussing recent European efforts to bolster regulations surrounding use of FRT).

[87] 105 N.Y.S.3d 794, 805-06 (Sup. Ct. 2019).

[88] *Id.* at 802-04.

if they are videotaped, and therefore, identify their children."[89] Accordingly, the mere availability of unregulated FRT programs was enough to deny filming the proceedings to protect "the non-consenting party, witnesses, attorneys, including attorneys for the children, and the children themselves."[90]

In the absence of judicially mandated limits, states have enacted legislation to bar the use of biometric products, particularly FRT, by law enforcement and state agencies. Maryland imposed warrant requirements for FRT searches.[91] Rhode Island considered a ban on drones with FRT, but the bill died in committee.[92] In 2019, California passed The Body Camera Accountability Act, which prevented the use of facial recognition by law enforcement agencies statewide.[93] In June 2020, a new bill was proposed that would provide a framework by which companies and government agencies could use facial recognition technology, provided they give notice.[94] Even cities have taken action. San Francisco banned police from using FRT.[95] Boston's city council unanimously passed an ordinance that barred the police and city officials from using facial recognition technology or obtaining facial surveillance from a third party, becoming the second-largest city in the world to do so.[96] As of now, Boston is one of seven municipalities in Massachusetts that have banned the use

[89] *Id.* at 804.

[90] *Id.* at 805. Judicial doctrines forged in a prebiometric world strongly support the expanding deployment and use of the technology. For example, courts have upheld the constitutionality of the DNA Analysis Backlog Elimination Act of 2000, which requires felons to submit blood samples from which authorities could obtain their DNA profile. *See* United States v. Kincade, 379 F.3d 813, 840 (9th Cir. 2004).

[91] S.B. 649, 2020 Leg., 441st Sess. 2020 (Md. 2020) (requiring custodian of records for Maryland Motor Vehicle Administration to deny inspection by ICE unless custodian is provided with valid warrant or subpoena).

[92] H. 7756, 2018 Gen. Assemb., Jan. Sess. (R.I. 2018).

[93] Assemb. B. 1215, 2019-2020 Leg., Reg. Sess. (Cal. 2020); *see also* Tristan Greene, *California Bans Law Enforcement from Using Facial Recognition Software for the Next 3 Years*, TNW (Oct. 9, 2019), https://thenextweb.com/artificial-intelligence/2019/10/10/california-bans-law-enforcement-from-using-facial-recognition-software-for-the-next-3-years/ [https://perma.cc/994M-6BGQ].

[94] Assemb. B. 2261, 2019-2020 Leg., Reg. Sess. (Cal. 2020); *see also* Russell Brandom, *California's Statehouse Is Considering a Controversial Facial Recognition Bill*, VERGE (June 3, 2020, 4:46 PM), https://www.theverge.com/2020/6/3/21279539/california-facial-recognition-ab2261-law-privacy-regulation. The American Civil Liberties Union ("ACLU") criticized this bill for undermining previous California law, noting that the bill made it "too easy to scan a user's face without their permission, with no consent required for government agencies and only minimal requirements for businesses." Brandom, *supra*.

[95] *See* Kate Conger, Richard Fausset & Serge. F. Kovaleski, *Tech-Savvy City Bans a Crime-Fighting Tool: Facial Recognition*, N.Y. TIMES, May 15, 2019, at A1.

[96] Amer Owaida, *Facial Recognition Technology Banned in Another US City*, WELIVESECURITY (June 25, 2020, 5:35 PM), https://www.welivesecurity.com/2020/06/25/boston-facial-recognition-technology-banned-another-us-city/ [https://perma.cc/M8N9-36WN].

of facial recognition technology, the others being Springfield, Cambridge, Northampton, Brookline, Somerville, and Easthampton.[97] On the federal level, lawmakers have introduced a bill that would make it "unlawful for any Federal agency or Federal official, in an official capacity, to acquire, possess, access, or use . . . any biometric surveillance system . . . or . . . information derived from a biometric surveillance system" in the United States.[98] Yet, these measures are largely ineffectual as biometric products and their use are expanding exponentially.[99]

FRT, and biometric technology more generally, presents a quantum shift for privacy theory. Because FRT operates in public, it falls into an area long treated as warranting minimal expectations of privacy. Indeed, FRT fulfills long-standing concerns over privacy protections tied to "reasonable expectations of privacy" of individuals as first stated in *Katz v. United States*.[100] The generally accepted understanding of *Katz* limits police surveillance to the extent that it contravenes such expectations of privacy. Thus, as expectations of privacy in society fall, the permissible scope of warrantless government surveillance increases. As warrantless surveillance increases, expectations fall further. FRT represents an accelerant for this trend in getting citizens to not only accept but welcome a nonymous society where they are recognized in stores and on the streets.

This Article shows that FRT also evades the legal protections based on property theories because there is no need to trespass or attach devices to private property. It is a technology that is perfectly suited to evade privacy protections. For those worried about a post-privacy world, FRT and other biometric technology could well be the expanding portal to that dystopia. This technology is rapidly transforming a society predicated on privacy into a fishbowl society where identity and transparency are defining elements. In England, police are handing out free Ring door cameras (which can record video accessible to the

[97] Douglas Hook, *Easthampton Is the Latest Massachusetts Community to Pass a Municipal Ban on Facial Recognition Technology*, MASSLIVE (July 2, 2020), https://www.masslive.com/news/2020/07/easthampton-is-the-latest-massachusetts-community-to-pass-a-municipal-ban-on-facial-recognition-technology.html [https://perma.cc/N6YA-T8LP].

[98] Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. § 3(a) (2020); *accord* Charlotte Jee, *A New US Bill Would Ban the Police Use of Facial Recognition*, MIT TECH. REV. (June 26, 2020), https://www.technologyreview.com/2020/06/26/1004500/a-new-us-bill-would-ban-the-police-use-of-facial-recognition/ [https://perma.cc/Z67D-K3RF].

[99] *See* Luana Pascu, *Global Biometrics Market to Surpass $45B by 2024, Reports Frost & Sullivan*, BIOMETRICUPDATE.COM (Mar. 20, 2020), https://www.biometricupdate.com/202003/global-biometrics-market-to-surpass-45b-by-2024-reports-frost-sullivan [https://perma.cc/CC6M-LZRQ] (highlighting rapid developments in biometric trends and compound annual growth rate of 19.6% in global biometrics market).

[100] 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

police),[101] conducting surveillance trials at public shopping centers,[102] and fining individuals who try to cover or obscure their faces from FRT-equipped cameras.[103] The CIA is reportedly working on deploying FRT that can be used from drones or long distances.[104] Being part of the mob was once a mask, but the mask has been lifted with this technology. This Article explores not only this technology and its capabilities but also how we define the privacy issues raised by the pervasive recognition in society.

Much of the existing case law has focused on an ill-defined right to privacy, a right that seems to largely dissipate in public. Not only is FRT designed principally to be used in public but also it forces a new conception of biometric privacy: one's interest in not being monitored through one's facial, physical, and behavioral characteristics. Biometric privacy is not about protecting something withheld but something ubiquitous. In that sense, it is a species more of a right to anonymity than conventional privacy. An anonymity model captures not just a different set of interests but interests that rest with society as well as the individual.

There is of course a danger that—as an extension of privacy—anonymity might become something of a tautology that is valued because it is valuable. The true value of anonymity is that it allows people to participate in essential democratic activities, such as associations and advocacy, without fear of reprisal. It is not sufficient to protect the marketplace of ideas if citizens are afraid of actually going to the marketplace for fear of recognition, tracking, and judgment. While superior to the privacy model, the anonymity model suffers from the simple reality that recognition technologies are being readily embraced by both citizens and businesses.

This Article explores these questions in four parts. Part I looks at the quantum shift of biometrics from prior periods of surveillance. Technology has driven much of our privacy rules and case law. This evolution is explored from the earliest eavesdropping practices to electronic interception to the new biometric period. The evolving technology defined not just the threat to privacy but also

---

[101] Tariq Tahir, *Police Team Up with Amazon Ring to Hand Out Free Camera Doorbells Worth £89 to Thousands of Households Across Britain*, SUN (Sept. 9, 2019, 3:13 PM), https://www.thesun.co.uk/news/9886618/police-amazon-free-camera-doorbells/ [https://perma.cc/BAM6-WV3H].

[102] Damien Gayle, *Privacy Campaigners Warn of UK Facial Recognition 'Epidemic*,*'* GUARDIAN (Aug. 16, 2019, 7:49 AM), https://www.theguardian.com/technology/2019/aug/16/privacy-campaigners-uk-facial-recognition-epidemic [https://perma.cc/CVU5-HKJ5].

[103] Zoe Drewett, *Moment Man Is Fined £90 for Hiding Face from Police Facial Recognition Cameras*, METRO (May 16, 2019, 1:24 PM), https://metro.co.uk/2019/05/16/moment-man-fined-90-hiding-face-police-facial-recognition-cameras-9571463/.

[104] Jack Corrigan, *The Intelligence Community Is Exploring Long-Range Biometric Identification*, NEXTGOV (Sept. 16, 2019), https://www.nextgov.com/emerging-tech/2019/09/intelligence-community-exploring-long-range-biometric-identification/159907/ [https://perma.cc/MCT2-7RUF].

the societal definitions of privacy. Privacy concepts have been forged around various dynamics or dichotomies from the public/private distinctions to the decisional/informational distinctions. Biometric technology exacerbates the weakness of these distinctions as a foundation for privacy protections. This is a technology designed to be used in public areas without the knowledge—let alone the consent—of individuals.

Part II suggests that the difficulty in addressing biometric technology is due to a lack of consensus on what we are trying to protect. Addressing biometrics judicially or legislatively will require a better understanding of what we are seeking to shield from exposure. Neither normative nor law enforcement perspectives can address the concerns raised by such transparency-forcing technology. If left to traditional views of privacy (including its general rejection of the concept of public privacy), biometric technology could expand exponentially and create the type of fishbowl or post-privacy world that civil libertarians have long feared. Instead, this Article suggests that the focus of biometric privacy should be the protection of democratic values of speech and association in public. Applying sociological and psychological research, it explores how observation changes human behavior and how biometric technology could radically deter the formation of viewpoints and associations vital to a democratic system.

Part III turns to anonymity rather than privacy as the possible focus of limitations on this technology. Anonymity comes closer to capturing the value that civil libertarians seek to protect: allowing people to move in public without recognition or potential tracking. As noted, the problem with anonymity as the focus for biometric privacy is that we are increasingly living in a nonymous rather than an anonymous society. This is due to a myriad of products and practices embraced by consumers that use FRT and other biometric technology. Accordingly, this Article concludes that it is not anonymity but obscurity that should be the focus of biometric privacy. The idea is that we can protect democratic values of public association and interactions by obscuring recognition even in an otherwise nonymous society. In this way, a right to obscurity in public movements can help create and maintain the type of bounded rationality needed for democratic expression and associations.

Finally, Part IV lays out the constitutional, statutory, and common-law means for the protections of such biometric privacy values.[105] It draws an analogy to the drafting of an omnibus law on electronic surveillance, which came after the Supreme Court defined privacy protections with the expansion of electronic surveillance. Biometric technology requires an even more fundamental reconsideration of the interests that we need to protect in public as well as new

[105] In a subsequent article, I will explore the specific provisions and programs necessary for the creation of this type of public private space. Jonathan Turley, From Here to Obscurity: Codifying Biometric Privacy for a Nonymous Society (Nov. 1, 2020) (unpublished manuscript) (on file with the Boston University Law Review) [hereinafter Turley, From Here to Obscurity].

means to carve out areas of anonymity by obscurity in public movements and associations.

This approach clearly does not seek a codification of the type of normative view of privacy that many of us hold. However, as John Dewey once argued, individual rights need not be recognized as the immutable possessions of individuals to achieve protection in society.[106] They can be justified on an instrumental level for "the contribution they make to the welfare of the community."[107] To put it simply, the libertarian privacy community is losing this battle to biometrics by arguing purely on normative grounds. Just as generals are often accused of planning to fight the last war, civil libertarians are clinging to past models despite those ideas' decreasing relevance as applied to contemporary technologies. This Article seeks to focus reforms on the instrumental role of anonymity—or, more properly, obscurity—in our democratic system.

I. PARADIGM SHIFTS IN PRIVACY FROM EAVESDROPPING TO BIOMETRICS

The biometric revolution represents a new and unique period of surveillance. Unlike prior periods, this new industry is not the result of simple breakthrough technology as was the case with wiretaps or nontrespassory listening devices. Biometric technology represents the marriage of surveillance technology (including some previously available technology) and information technology, allowing for rapid and accurate identification of individuals. Most importantly, this technology is designed in large part to operate in public, using publicly available images or data. It is not surreptitious but exploitative technology that uses information exposed by individuals in the public realm. In this way, the biometric profile represents a perfect storm for privacy advocates: (1) a new technology, (2) used in public forums, (3) that allows for immediate identification and tracking of large numbers of individuals. To understand why biometric technology represents such a challenge legally, it is useful to examine the historical struggle between privacy and technology in the law. Surveillance history can be generally grouped into three phases characterized by the unique tension between privacy law and technology as societies have moved from eavesdropping to interception and now to biometrics. These phases are (1) the eavesdropping period, (2) the interception period, and (3) the biometric period. Each period is considered in turn, below.

A. *The Eavesdropping Period*

From the earliest forms of government, officials developed an insatiable appetite for information. Eavesdropping was a common and largely nonconsensual practice, its name stemming from the act of standing in the eaves

[106] JOHN DEWEY, LIBERALISM AND CIVIL LIBERTIES (1936), *reprinted in* 11 JOHN DEWEY, THE LATER WORKS, 1925–1953, at 372, 373 (Jo Ann Boydston ed., S. Ill. Univ. Press 2008).

[107] *Id.*

to monitor the conversations within a room.[108] Indeed, in the Sicilian city of Syracuse, one of earliest forms of surveillance technology permitted such eavesdropping by luring prisoners into a false sense of privacy. It consisted of a large, S-shaped cave, called the "Ear of Dionysius" that was perfect for allowing captors located at the mouth of the cave to listen to the conversations of captive prisoners.[109] Such early cases concerned surreptitiously listening.[110] By secreting oneself in a hidden corner or an eave, one could gather confidential information. Alternatively, it was possible to acquire the same information as a so-called false friend—i.e., an informant. The earliest cases rejected claims that the law can protect people from false friends.[111]

That did not mean that there were no protections against eavesdropping. Those protections were largely against neighbors rather than the government, and the cause of action was found in nuisance. Sir William Blackstone described eavesdropping as "listen[ing] under walls or windows or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales."[112] These cases were precursors to the modern tort of intrusion upon seclusion and reflect a more instrumental (rather than immutable) notion of privacy. Constant vulnerability to interlopers and eavesdroppers prevented people from enjoying their home. The emphasis on the framing of "slanderous and mischievous tales" reflects the type of tortious injuries that comes from such eavesdropping.[113]

While allowing nuisance actions, the United States followed this limited view of privacy protections against the U.S. government. In *On Lee v. United States*,[114] a government informant, Chin Poy, engaged On Lee in a conversation while wearing a microphone.[115] The Supreme Court reaffirmed that the Fourth Amendment does not protect against being overheard, even with the aid of a microphone. The Court rejected the idea that such fraudulent intrusions into private conversations were constitutional violations.

> This was due to aid from a transmitter and receiver, to be sure, but with the same effect on his privacy as if agent Lee had been eavesdropping outside

[108] JOHN L. LOCKE, EAVESDROPPING: AN INTIMATE HISTORY 17 (2010).

[109] *See* NAT'L COMM'N FOR THE REVIEW OF FED. & STATE LAWS RELATING TO WIRETAPPING & ELECTRONIC SURVEILLANCE, ELECTRONIC SURVEILLANCE 33 (1976), https://www.ncjrs.gov/pdffiles1/Digitization/39007NCJRS.pdf [https://perma.cc/8P8Y-TYMX]; Jonathan Turley, *The Not-So-Noble Lie: The Nonincorporation of State Consensual Surveillance Standards in Federal Court*, 79 J. CRIM. L. & CRIMINOLOGY 66, 74 n.43 (1988) [hereinafter Turley, *The Not-So-Noble Lie*]; *see also* K.A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J.L. & TECH. 128, 141 (2007).

[110] Turley, *The Not-So-Noble Lie*, *supra* note 109, at 74-75.

[111] *Id.* at 74; *see also, e.g.*, On Lee v. United States, 343 U.S. 747, 757 (1952).

[112] 5 WILLIAM BLACKSTONE, COMMENTARIES 168 (St. George Tucker ed., 1803).

[113] *See id.*

[114] 343 U.S. 747 (1952).

[115] *Id.* at 749.

> an open window. The use of bifocals, field glasses or the telescope to magnify the object of a witness' vision is not a forbidden search or seizure, even if they focus without his knowledge or consent upon what one supposes to be private indiscretions. It would be a dubious service to the genuine liberties protected by the Fourth Amendment to make them bedfellows with spurious liberties improvised by farfetched analogies which would liken eavesdropping on a conversation, with the connivance of one of the parties, to an unreasonable search or seizure. We find no violation of the Fourth Amendment here.[116]

The Court's decision highlighted Fourth Amendment jurisprudence's transition to the trespass doctrine. With the advent of transmitting and recording technology, eavesdropping was no longer a matter of a false friend but of a captured conversation. The courts, however, clung to the notion that there was no privacy protection for consensual conversations absent some collateral offense like trespass. The Supreme Court agreed.

> Petitioner relies on cases relating to the more common and clearly distinguishable problems raised where tangible property is unlawfully seized. Such unlawful seizure may violate the Fourth Amendment, even though the entry itself was by subterfuge or fraud rather than force. But such decisions are inapposite in the field of mechanical or electronic devices designed to overhear or intercept conversation, at least where access to the listening post was not obtained by illegal methods.[117]

Thus, privacy concerns in the eavesdropping period focused on "unlawfully seized" material, not the loss of an expectation of privacy due to the "subterfuge" of a government agent.[118] Hence, when a government agent stole material from a target's office in *Gouled v. United States*,[119] the Court saw a violation of the Fourth Amendment.[120] The Court was protecting a criminal justice line between the individual and their government in such capture of property as opposed to words.

B. *The Interception Period*

As evidenced by *On Lee*, the classic eavesdropping case gradually transformed with technology. Just as transmitters were used to allow others to eavesdrop on consensual conversations, they soon allowed for the placement of microphones in rooms without the need of a third party. This period can be loosely referenced as the interception period, reflecting the most significant technological development from the eavesdropping baseline. The advent of wire communications (first in the invention of the telegraph and then of the telephone)

---

[116] *Id.* at 754.

[117] *Id.* at 753 (citations omitted).

[118] *Id.*

[119] 255 U.S. 298 (1921).

[120] *Id.* at 313.

and the subsequent use of "wiretapping," a term still used by some to refer to surveillance,[121] represented a significant shift from earlier rudimentary listening techniques. During the Civil War, a large number of Union and Confederate soldiers were trained in both wire communications and interception.[122] After the war, those soldiers found their skills in high demand. Business, media, and the government quickly capitalized on the vulnerability of wire communications to splicing and tapping measures. The result was a surge of unregulated surveillance.

The Supreme Court played a curious role in the evolution of interception technology with its creation of the trespass doctrine. It finally addressed telephone interceptions in 1928 in *Olmstead v. United States*.[123] Nominally involving violations of the National Prohibition Act, the prosecution's case was built on the interception of telephone messages. In rendering a verdict, the Court remained mired in the past context of privacy cases—focusing on the objects of surveillance rather than the underlying privacy interest. It seemed incapable of acknowledging the paradigm shift occurring under its very feet.

> It is plainly within the words of the [Fourth] Amendment to say that the unlawful rifling by a government agent of a sealed letter is a search and seizure of the sender's papers or effects. The letter is a paper, an effect, and in the custody of a Government that forbids carriage except under its protection.
>
> The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. . . . The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.
>
> By the invention of the telephone, fifty years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place. The language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched.[124]

---

[121] In a recent example, President Donald Trump was criticized for insinuating that the Obama Administration had possibly "wiretapped" his presidential campaign officials. *See* Brett Samuels, *Trump: Claim of Obama Wiretapping Based 'on a Little Bit of a Hunch,'* HILL (Apr. 25, 2019, 10:00 PM), https://thehill.com/homenews/administration/440778-trump-says-2017-claim-of-obama-wiretapping-was-based-on-a-little-bit [https://perma.cc/XKU7-3GX3]. While some took that as a literal reference to a wiretap placed on campaign phones, many in President Trump's generation were raised with "wiretapping" as the term for government surveillance.

[122] Turley, *The Not-So-Noble Lie*, *supra* note 109, at 74-75.

[123] 277 U.S. 438, 455 (1928) (determining "whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wire tapping" violated the Fourth and Fifth Amendments).

[124] *Id.* at 464-65.

The Court reaffirmed this narrow approach in *Goldman v. United States*.[125] In *Goldman*, the government used an actual listening device against a wall to gather evidence of criminal fraud.[126] The original device was placed in a tiny opening in the shared wall with an adjoining office, but it failed to work. The federal agents then proceeded to use a "detectaphone" that was placed against the wall to listen through it.[127] A stenographer sat in the adjoining office and typed up the overheard conversation. The Court ruled that there was no meaningful difference between the actions taken in *Olmstead* and *Goldman* in terms of trespass law and thus found no Fourth Amendment violation.[128] Although Justice Brandeis had dissented from the majority's "impotent and lifeless formulas" in *Olmstead*,[129] the *Goldman* majority remained wedded to its outdated and increasingly absurd doctrine. The resulting case law provided a judicial incentive for the market to create nontrespassory surveillance devices. Surveillance flourished under the archaic views of the Supreme Court as both oral and wire communications were intercepted with increased ease and accuracy.

The "impotent and lifeless" trespass doctrine theoretically met its end in the famous *Katz* decision when Justice Brandeis's view finally prevailed. The Court made a second paradigm shift in declaring that "the Fourth Amendment protects people, not places."[130] In his majority opinion, Justice Stewart established that "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.'"[131] In his concurrence, Justice Harlan expanded on this notion when he articulated the now famous test that "there is a twofold requirement [to establish a right to privacy], first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[132] Privacy had finally prevailed over technology and was largely decoupled from arbitrarily determinative locational elements.

Yet, there are exceptions to this paradigm shift. The Court continued its locational analysis in one important respect: public disclosures and conduct. The Court has consistently drawn a line on the expectation of privacy, and that line generally ends when one enters the public. This was evident in two foundational cases: *United States v. Karo*[133] and *United States v. Knotts*.[134] Both cases

[125] 316 U.S. 129, 135-36 (1942) (finding no Fourth Amendment violation when federal agents installed listening device on other side of defendants' office wall).

[126] *Id.* at 131-32.

[127] *Id.*

[128] *Id.* at 135.

[129] *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).

[130] Katz v. United States, 389 U.S. 347, 351 (1967).

[131] *Id.* at 350.

[132] *Id.* at 361 (Harlan, J., concurring).

[133] 468 U.S. 705 (1984).

[134] 460 U.S. 276 (1983).

involved public elements tied to new technology. In each case, the police placed hidden beeper devices to track subjects. In *Karo*, the Court rejected the use of a tracking device that allowed the police to follow the suspect's movements after the device was within a house.[135] However, in *Knotts*, the Court approved the police tracking what "amounted principally to the following of [the suspect's] automobile on public streets and highways."[136] Thus, the expectation of privacy recognized in *Karo* effectively ended at the threshold of the suspect's home. Once in public, the suspect in *Knotts* was viewed as having little or no expectation of privacy because he *could have been* observed by the naked eye. As discussed below, the Supreme Court would return to this property-based protection for surveillance in *United States v. Jones*[137] by declaring that a GPS device placed on a vehicle was unconstitutional.[138] Notably, the Supreme Court's narrow rationale in *Jones* did not rely on the expectation of privacy in public movements, opting instead to base protection on the freedom from the invasion of private property.[139]

With the increased use of biometrics, we now have a technology that is based entirely on public observation without the need to touch a suspect or even be anywhere close to a suspect. Before confronting how this technology can be addressed in our existing privacy models, a brief discussion of the scope and capabilities of this technology is warranted. This includes a discussion of the primary nonprivacy objection to biometric (and specifically FRT) systems.

C. *The Biometric Period*

1. Early Biometric Identification

On one level, the use of biometrics is just a continuation of a long effort to establish reliable identification systems. The use of composite artists, mugshots, and other crude systems is readily accepted as a legitimate function of the police. Creating a record of criminals' faces goes back to the mid-nineteenth century. Both Liverpool and Birmingham police began photographing criminals in

[135] *Id.* at 718.

[136] *Knotts*, 460 U.S. at 281.

[137] 565 U.S. 400 (2012).

[138] *Id.* at 404 (holding that physical intrusion of defendant's vehicle to place device constituted search under Fourth Amendment).

[139] *Id.* For a more in-depth discussion of *Jones*, see *infra* notes 243-51 and accompanying text.

1848.[140] By 1857, the New York Police Department was archiving mugshots.[141] The typical full face and profile shots appeared in 1888 in Paris through the efforts of photographer Eugene Appert and French police officer Alphonse Bertillon.[142] These daguerreotypes were early efforts to create systems for identification. With the advent of computers, such mugshots could be easily shared. Modern programs now allow rapid facial recognition by running a crime scene photo against a national databank. People have long accepted the use of such images in wanted posters and the issuance of all-points bulletins with pictures for officers.

Fingerprinting was also a forerunner to modern biometrics. Since Babylonian times, fingerprints were recognized as a reliable form of identification.[143] Similar systems were used in ancient China.[144] By 1684, Dr. Nehemiah Grew completed a study for London's Royal Society detailing the ridges and pores on an individual's hands and feet.[145] It was roughly 100 years later that J.C.A. Mayer posited the theory that fingerprints are unique to each person.[146] In 1858, Sir William Herschel established the value of using this method to identify criminal suspects in India.[147] The first public study was published a couple decades later by Sir Francis Galton at the urging of his cousin Charles Darwin.[148] However, the most interesting of these early pioneers was Alphonse Bertillon, who pursued early means of biometric measurements from heat to foot measures.[149] This use of anthropometry was revolutionary and spread rapidly among police departments. By the turn of the twentieth century, Metropolitan Police Commissioner Sir Edward Henry had developed a more sophisticated classification system.[150] As a result, Scotland Yard officially opened the first

[140] *See* Dominic Midgley, *World's First Ever Mugshots – an Early Rogues Galley of 19th Century Criminals*, EXPRESS (June 14, 2018, 8:10 AM), https://www.express.co.uk/life-style/life/974039/mugshot-police-criminals-worlds-first-birmingham [https://perma.cc/8VLF-A5V7].

[141] *The NYPD's Pioneering 19th Century Mugshots*, EPHEMERAL N.Y. (May 26, 2014, 6:39 AM), https://ephemeralnewyork.wordpress.com/2014/05/26/the-nypds-pioneering-19th-century-mugshots/ [https://perma.cc/DYW5-5ADD].

[142] *See generally* Pierre Piazza, *Bertillonage: The International Circulation of Practices and Technologies of a System of Forensic Identification*, CRIMINOCORPUS (Apr. 18, 2011), https://journals.openedition.org/criminocorpus/2970?lang=en#text [https://perma.cc/E5B4-QVCR].

[143] *See* Vincent J. Gnoffo, *Requiring a Thumbprint for Notarized Transactions: The Battle Against Document Fraud*, 31 J. MARSHALL L. REV. 803, 806 (1998).

[144] *Id.*

[145] *See* ANNITA T. FIELD, FINGERPRINT HANDBOOK 3 (1959).

[146] *Id.* at 4.

[147] *Id.*

[148] *Id.* (noting that parts of Galton's material are still used in some areas of the world).

[149] HENRY T.F. RHODES, ALPHONSE BERTILLION: FATHER OF SCIENTIFIC DETECTION 71-129 (1956).

[150] FIELD, *supra* note 145, at 5.

fingerprint bureau based on the Henry Classification System in 1901.[151] Two years later, the New York Police Department created its fingerprinting system.[152] While modern fingerprinting technology has not developed truly remote collection systems, it has left the old ink-and-paper system far behind. Not only are fingerprints captured digitally, but new systems also allow for an all-digit acquisition in a fraction of a second when a hand is passed over a sensor. As this technology improves, the danger is that fingerprints may be acquired without consent or knowledge.[153]

Blood type has long been a feature in criminology. In the past, blood type was primarily used to eliminate suspects according to broad groups. It was not generally used as a means to identify an individual as much as it was used in conjunction with other evidence to better understand whether the individual could be the culprit. That changed in a major way with the advent of DNA fingerprinting, where blood (and later other biological sampling) could yield a virtually unique identification code.[154] First explored in the early 1980s, DNA fingerprinting has become a regular element in criminal trials.[155] While 99.9% of human DNA sequences are the same between individuals, the DNA analysis focuses on repetitive valuable sequences (called variable number tandem repeats) to identify individuals. The use of the term "DNA fingerprinting" by Alec Jeffreys reflected the obvious conceptual connection to dermatoglyphic

[151] *Id.*

[152] *Id.*

[153] This technology is not currently approved for use and would likely face barriers for adoption by U.S. law enforcement under the Appendix F certification process. *See generally* JENETRIC, FOUR STEPS FOR SELECTING THE RIGHT FBI FINGERPRINT CATEGORY, https://www.jenetric.com/fileadmin/user_upload/Guide_for_fingerpint_category_Whitepaper_JENETRIC.pdf [https://perma.cc/37ZQ-2PSG] (last visited Nov. 18, 2020) (explaining rigorous requirements for obtaining Appendix F certification). Systems like IDEMIA's MorphoWave are used with the volition of the subject. Luana Pascu, *Idemia Scanner Tops Contactless Fingerprint Biometrics in NIST Accuracy, Interoperability Test*, BIOMETRIC UPDATE (June 22, 2020), https://www.biometricupdate.com/202006/idemia-scanner-tops-contactless-fingerprint-biometrics-in-nist-accuracy-interoperability-test [https://perma.cc/CT2R-AUJB].

[154] Even DNA fingerprinting, however, is not absolutely unique. Monozygotic siblings (or identical twins) have essentially identical genomes with less random and infrequent mutations and comprise about 0.3% of live births. *Is the Probability of Having Twins Determined by Genetics?*, MEDLINEPLUS, https://medlineplus.gov/genetics/understanding/traits/twins [https://perma.cc/C29D-276F] (last visited Nov. 18, 2020); *see also* Zhenan Sun, Alessandra A. Paulino, Jianjiang Feng, Zhenhua Chai, Tieniu Tan & Anil K. Jain, *A Study of Multibiometric Traits of Identical Twins*, PROC. SPIE BIOMETRIC TECH. FOR HUM. IDENTIFICATION VII, Apr. 2010, at 5-10 (demonstrating the inability of commercial unimodal and multimodel biometric systems to accurately distinguish between identical twins when considering fingerprints, irises, and face prints).

[155] David L. Faigman, *The Tipping Point in the Law's Use of Science: The Epidemic of Scientific Sophistication that Began with DNA Profiling and Toxic Torts*, 67 BROOK. L. REV. 111, 116-17 (2001).

fingerprints in establishing a unique pattern that could dispositively establish identity.[156] Indeed, courts eventually concluded that the largest difference between genetic and dermatoglyphic fingerprinting was that the former was far more accurate.[157] With the collection of private and governmental companies, including the rising popularity of DNA testing for genealogical records, DNA fingerprinting is also part of the big data trend of collecting millions of such profiles.

Retinal and iris scans are another widely used form of biometrics. While iris scanning is more practical and popular, retinal scans capture the patterns of veins in the back of the eye. The use of near infrared light highlights the blood vessels located on the retina rather than its color and establishes patterns in the colored tissue around the center of the eye. This often depends on the cooperation of the subject because the technology operates at a range of about three to seven inches and requires proper positioning of the light and camera.[158] However, a retinal scan requires the subject to be inches away, while the iris scan can be done at a few meters and is capable of reading a subject who is moving.[159] The advantage of these eye scans is the ability to use them on computers and fixed cameras. They are also ideal for overlapping biometric identifications when used in combination with key stroke identification technology. Likewise, the government has used Mobile Offender Recognition and Identification System, allowing for a basic cell phone to capture both iris and face prints for overlapping biometric identifications.[160]

In addition to these dominant biometric systems, there are gait systems, which identify persons by their walking characteristics;[161] voice-recognition systems;[162] keystroke-recognition systems;[163] finger-and-palm-vein-recognition

[156] KEITH INMAN & NORAH RUDIN, AN INTRODUCTION TO FORENSIC DNA ANALYSIS 20 (1997).

[157] Maryland v. King, 569 U.S. 435, 451 (2013) ("[T]he only difference between DNA analysis and the accepted use of fingerprint databases is the unparalleled accuracy DNA provides."); *see also* Haskell v. Harris, 669 F.3d 1049, 1060 (9th Cir. 2012).

[158] *See generally* John Daugman, *Iris Recognition*, 89 AM. SCIENTIST 326 (2001); Nicholas Orlans, *Eye Biometrics: Iris and Retina Scanning*, *in* JOHN D. WOODWARD, JR., NICHOLAS M. ORLANS & PETER T. HIGGINS, BIOMETRICS 89, 91 (Sarah Granger ed., 2003).

[159] Orlans, *supra* note 158, at 91.

[160] Emily Steel, *How a New Police Tool for Face Recognition Works*, WALL STREET J. (July 13, 2011, 7:56 AM), https://www.wsj.com/articles/BL-DGB-22776.

[161] Imad Khan, *China Implements Tech that Can Detect People by the Way They Walk*, ENGADGET (Nov. 7, 2018), https://www.engadget.com/2018/11/07/china-implements-gait-recognition/ [https://perma.cc/MU2K-XEAK].

[162] Naveen Joshi, *Artificial Intelligence Powered Biometrics*, BBN TIMES (July 1, 2019), https://www.bbntimes.com/en/technology/artificial-intelligence-powered-biometrics [https://perma.cc/EE77-KFZA].

[163] *Id.* (stating that one's time spent searching for and pressing keys can "be calculated together to authenticate individuals").

systems;[164] and countless more in development. U.S. Special Forces have started using technology that can detect the unique cardiac signature of individuals with infrared lasers.[165] The cardiac signature devices are reporting a 95% accurate identification rate with a current range of 200 meters, although longer distances are technically possible.[166]

2. The Transformative Capacity of Biometric Technology

All of these systems are enhanced by new data storage and processing systems that allow for rapid comparisons with a subject's biometric identifications. This is accomplished by converting biometric characteristics into a series of ones and zeros for computer processing. For example, using MIT's "Eigenface" ("one's own face") technology, a person's face is captured in two dimensions with 100 to 125 "eigenfaces" (key characteristics) combined before being converted into numbers to be cross-checked against future efforts to gain access to a system.[167] New systems using Deep Convolutional Neural Networks radically enhance such processing and identification.[168] Like iris scans, many of these systems require proper framing to achieve high accuracy rates. Most systems extract this information through basic steps, starting with patterns from an image of a face. An algorithm then registers the face and places it into a preset position for comparison. This "face print" can then be compared to a data bank and stored for future authentication or identification purposes.

The accuracy of the most competitive FRT programs is remarkably high in top-performing systems. Testing of FRT is generally done with one-to-one image comparisons ("1:1") and one-to-many image comparisons ("1:N"). The most comprehensive testing has been performed by NIST, which has produced roughly two dozen reports. The number of algorithms and their accuracy have rapidly improved.

A 2017 competition hosted by NIST tested sixteen algorithms, while the testing conducted just the following year evaluated 127 algorithms from forty-

[164] Richard Adhikari, *Amazon Trying Out Hand-Scanning Payment System: Report*, TECHNEWSWORLD (Sept. 5, 2019, 3:11 AM), https://www.technewsworld.com/story/86225.html [https://perma.cc/U8RH-4RJW].

[165] David Hambling, *The Pentagon Has a Laser that Can Identify People from a Distance—by Their Heartbeat*, MIT TECH. REV. (June 27, 2019), https://www.technologyreview.com/s/613891/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/.

[166] *Id.*

[167] Matthew Turk & Alex Pentland, *Eigenfaces for Recognition*, 3 J. COGNITIVE NEUROSCIENCE 71, 71 (1991).

[168] *See* Bong-Nam Kang, Yonghyun Kim & Daijin Kim, *Deep Convolutional Neural Network Using Triplets of Faces, Deep Ensemble, and Score-Level Fusion for Face Recognition*, 2017 IEEE CONF. ON COMPUTER VISION & PATTERN RECOGNITION 611, 616-17.

one different developers.[169] The 2019 NIST testing involved nearly 200 such algorithms.[170]

Three algorithms were submitted for testing with 1:1 programs in February 2017, the best of which showed a 92% accuracy rate.[171] In the January 2019 test, NIST tested 189 algorithms, with the best performers hitting 99.6% accuracy rates.[172] The same pattern is evident for 1:N programs. NIST's 2018 testing found that "the most accurate algorithm [in 2018 was] substantially more accurate than anything reported [in the preceding eight years of testing]."[173] Specifically, the 2018 test noted a six-fold improvement in accuracy over the 2014 data for the top performing algorithm.[174] These tests show that many algorithms for both 1:1 (verification) programs and 1:N (identification) programs now routinely identify individuals with rates of accuracy over 99%.[175] There remains, however, the lingering controversy over a pattern of inaccuracy linked to race that was evident in some of the early algorithms.

One of the most common criticisms of FRT is that it produces a higher percentage of false matches in cases involving racial and ethnic minorities, particularly with other minority individuals. The FBI previously acknowledged a 15% error rate in its FRT programs.[176] Private programs have also shown

[169] PATRICK GROTHER, MEI NGAN, KAYEE HANAOKA, CHRIS BOEHNEN & LARS ERICSON, THE 2017 IARPA FACIAL RECOGNITION PRIZE CHALLENGE (FRPC) 2 (2017) [hereinafter NIST 2017 FACIAL RECOGNITION CHALLENGE], https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8197.pdf [https://perma.cc/A8HU-MVY5]; PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT), PART 2: IDENTIFICATION 2 (2019) [hereinafter NIST 2018 TEST], https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf [https://perma.cc/6WZ9-PXU4].

[170] PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT), PART 3: DEMOGRAPHIC EFFECTS 1 (2019) [hereinafter NIST 2019 DEMOGRAPHIC EFFECTS TEST], https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/4CNB-BREA].

[171] PATRICK GROTHER & MEI NGAN, NAT'L INST. OF STANDARDS & TECH., ONGOING FACE RECOGNITION VENDOR TEST (FRVT), PART 1: VERIFICATION 3 (2017).

[172] NIST 2019 DEMOGRAPHIC EFFECTS TEST, *supra* note 170; *see also* Sophie Bushwick, *How NIST Tested Facial Recognition Algorithms for Racial Bias*, SCI. AM. (Dec. 27, 2019), https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/ [https://perma.cc/4ZMT-EGVJ].

[173] NIST 2018 TEST, *supra* note 169.

[174] *Id.* at 37. The algorithm, created by a Shanghai corporation, Yitu Technology, was the top performer in the 2017. NIST 2017 FACIAL RECOGNITION CHALLENGE, *supra* note 169, at 10.

[175] NIST 2018 TEST, *supra* note 169 at 46.

[176] What is curious about this error rate is that the FBI has rights to algorithms with a 99% accuracy rate but did not update those systems. *See Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 4-5 (2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services, FBI). As noted earlier, the top-performing

concerning error rates, leading some, like Senator Bernie Sanders, to call for a ban on all law enforcement use of FRT,[177] while others call for a total ban on all FRT products.[178]

There have been studies, including more recent ones, showing that false identifications remain a problem. This concern was most notably raised in 2018 by the ACLU, which took Amazon's "Rekognition" system and ran the faces of the members of Congress against 25,000 mugshots, producing what it claimed were twenty-eight false matches.[179] In August 2019, the ACLU performed the same test with Amazon's product, this time using a database of 25,000 criminal mugshots and the California state legislature.[180] It reported twenty-six matches of legislators with various mugshots. In addition to claiming that the FRT program mismatched one in five legislators, the ACLU further reported that more than half were people of color.[181] Such studies, however, can be intentionally or negligently distorted to produce either high rates of accuracy or high rates of error.[182] By using low-performing algorithms or choosing a more

algorithms allow for less than a 1% error rate. NIST 2018 TEST, *supra* note 169 at 46; *see also* GROTHER, NGAN & HANAOKA, *supra* note 33, at 6.

[177] Donie O'Sullivan, *Bernie Sanders Wants to Stop Police from Using Facial Recognition Software*, CNN BUS. (Aug. 19, 2019, 1:59 PM), https://www.cnn.com/2019/08/19/tech/bernie-sanders-facial-recognition-police/index.html [https://perma.cc/A4JE-MDRF].

[178] Max Read, *Why We Should Ban Facial Recognition Technology*, N.Y. MAG.: INTELLIGENCER (Jan. 30, 2020), https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html [https://perma.cc/PT8Y-JFT3].

[179] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/DR4D-974S]; *see also* Matt Wood, *Thoughts on Machine Learning Accuracy*, AWS: NEWS BLOG (Jul. 27, 2018), https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/ [https://perma.cc/P6S9-4RQ9] (assuming that ACLU used the default threshold of 80% accuracy).

[180] Anita Chabria, *Facial Recognition ID'd Lawmakers as Crooks, ACLU Says*, L.A. TIMES, Aug. 13, 2019, at B1.

[181] Press Release, ACLU N. Cal., Facial Recognition Technology Falsely Identifies 26 California Legislators with Mugshots (Aug. 13, 2019), https://www.aclunc.org/news/facial-recognition-technology-falsely-identifies-26-california-legislators-mugshots [https://perma.cc/X53K-9JTT].

[182] The most-cited study raising the racial discrimination issue was produced by MIT and Stanford researchers. It found a pattern of algorithmic bias in relation to women and racial and ethnic minorities. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 CONF. ON FAIRNESS ACCOUNTABILITY & TRANSPARENCY, Feb. 2018, at 1, 10-12. I discuss this study and more recent countervailing studies in Turley, From Here to Obscurity, *supra* note 105. Many companies have tweaked their systems to address this problem and claim to have a much smaller error rate for dark-skinned females in current systems. An example of the new systems was highlighted by Ruchir Puri, CTO and Chief Architect of IBM Watson. Puri acknowledged the error rates in some prior programs. Using a diverse group of roughly the same amount of

uniform group, the results can vary.[183] Yet, as shown in the most recent NIST testing, the top performing 1:1 algorithms now perform better on Black men than on White men and women.[184] The results will vary significantly based on the selection of high- or low-performing algorithms.

As noted earlier, recent studies suggest that there are continuing problems in addressing these false positives or other errors among subjects, in particular among ethnic or racial groups. Some of these criticisms focus on earlier algorithms with lower "confidence" level selections.[185] The ACLU study using Rekognition, for example, is somewhat suspect in the criteria and program used. The ACLU appears to have set the threshold for identification at 80%.[186] This is substantially below the performance of the best algorithms, which are capable of operating at confidence rates as high as 99%.[187] Studies have established how different approaches can mitigate or eliminate the disparity. One such approach uses 3D face recognition by taking an image in poor conditions or lighting and extrapolating from the base image using modeling. A 3D modeling engine allows for a face to be placed in different poses to better match images and allows the viewer to rotate the model for a closer inspection.[188] Although the study correctly identified a serious concern with FRT systems, the current generation of programs has clearly made strides in correctly identifying within the groups of subjects historically misidentified, particularly dark-skinned women. Moreover, NIST is implementing a new standardized test to avoid such questions over the conditions set by researchers.

The most recent NIST study in December 2019 used roughly 200 facial recognition algorithms from ninety-nine developers to analyze over 18 million images from federal databases.[189] NIST found that the most accurate 1:1 algorithms had error rates below 1% "for almost all countries and demographic

subjects as the MIT study and breaking the group down into gender and skin color groups, Puri tried to replicate the results of the MIT study. Instead of recreating the 16.97% error rate in the study, Puri found that the new program had an error rate of 3.46%. Ruchir Puri, *Mitigating Bias in AI Models*, IBM: RES. BLOG (Feb. 6, 2018), https://www.ibm.com/blogs/research/2018/02/mitigating-bias-ai-models/ [https://perma.cc/6ZA2-SCHD].

[183] I address these concerns and a possible legislative precaution in another work. *See* Turley, From Here to Obscurity, *supra* note 105, at 29-30.

[184] NIST 2019 DEMOGRAPHIC EFFECTS TEST, *supra* note 170, at 63.

[185] A demand by U.S. House members to bar funding for any FRT was based on the 2018 ACLU report, which surveyed long-outdated products. Jim Nash, *Letter to Pelosi: Cut Facial Recognition Spending from Appropriation Bills*, BIOMETRIC UPDATE (July 23, 2020), https://www.biometricupdate.com/202007/letter-to-pelosi-cut-facial-recognition-spending-from-appropriation-bills [https://perma.cc/QB5W-HGAC].

[186] *See* Wood, *supra* note 179.

[187] *Id.*

[188] *See generally* Volker Blanz & Thomas Vetter, *Face Recognition Based on Fitting a 3D Morphable Model*, 25 IEEE TRANSACTIONS ON PATTERN ANALYSIS & MACHINE INTELLIGENCE 1063 (2003).

[189] NIST 2019 DEMOGRAPHIC EFFECTS TEST, *supra* note 170, at 1-11.

groups."[190] However, it still found varying degrees of accuracy with the highest error rates among Indigenous, Black, and Asian populations.[191] Women also experienced a higher error rate than men.[192] Top products did not show the same level of "demographic differences," and products developed in China notably did not show the same bias for East Asian people.[193] Thus, the study showed that such differences can be largely eliminated. Yet, "bias" remains the primary challenge for the industry and the overriding and legitimate concern of society.[194]

The NIST results have been widely reported and widely misconstrued. Demographic differences still remain a major concern, but the differential rate is very small among the leading algorithms, which should be the obvious choice for government agencies. Industry experts have noted that among seventeen of the top products,

> verification algorithms had similar levels of accuracy for black females and white males: false-negative rates of 0.49 percent or less for black females (equivalent to an error rate of less than 1 in 200) and 0.85 percent or less for white males (equivalent to an error rate of less than 1.7 in 200).[195]

It is principally among the worst performers that the performance has been described as a virtual "coin toss."[196] The study shows the need for greater regulation on performance, but it also shows that top algorithms can operate at a level that is extremely accurate and far beyond the capability of human performance.[197]

The use of FRT and other biometric systems represents a quantum leap in identification systems that could not only enhance law enforcement but also reduce false arrests as well as identity theft. Moreover, it is a technology that is embraced by consumers in a growing variety of products. Like any technology, it can also be abused. Yet, the parameters and confidence levels for FRT are

---

[190] *Id.* at 58.

[191] *Id.* at 2.

[192] *Id.*

[193] *Id.* at 7.

[194] *Id.* at 15.

[195] MICHAEL MCLAUGHLIN & DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., THE CRITICS WERE WRONG: NIST DATA SHOWS THE BEST FACIAL RECOGNITION ALGORITHMS ARE NEITHER RACIST NOR SEXIST 2 (2020).

[196] INT'L BIOMETRICS + IDENTITY ASS'N, NIST REPORT ON FACIAL RECOGNITION: A GAME CHANGER 3 (2020).

[197] *Id.* at 3 ("The most accurate high-performing identification algorithms . . . display virtually 'undetectable' differences among demographic groups; more than 30 of the 189 identification algorithms NIST tested have false non-match rates (misses) less than three per thousand, providing far greater accuracy than humans could ever achieve." (emphasis omitted) (footnotes omitted)).

subject to debate and alteration to address operational or training errors.[198] Ironically, the greatest danger of FRT is not its inaccuracy, but its accuracy. Programs routinely reach a 99% recognition rate—a success level that threatens to expose all citizens to continual monitoring of moves and associations in public.

II. BIOMETRIC PRIVACY UNDER PREBIOMETRIC RATIONALES

While the common criticism of FRT as inherently racially discriminatory is difficult to square with current research and testing, there remains the well-founded fear of the impact of FRT and biometric technology on privacy interests. This debate again presents countervailing values in the law enforcement context. On one hand, biometrics, when properly used, can enhance privacy interests and even reduce racial bias in policing, decreasing false arrests and unwarranted *Terry* stops.[199] Bans, like the one in San Francisco,[200] not only deny police a technology widely used by businesses but also return police to the highly flawed default of eyeballing suspects, where the error rate is considerably higher than top FRT programs.

An Australian study of passport officers offers a glimpse into the performance differential between human and FRT recognition. It showed high error rates, including a 14% false acceptance rate in testing.[201] What was striking was that the test used photos of the testing subjects taken in optimal settings just two days before they appeared before the officers. The variables of aging and poor images were therefore not present to the same degree as in real life. Nevertheless, the

[198] A good example of the training element is found in the controversy surrounding the arrest of Robert Williams, a Black man, in Detroit. Nancy Kaffer, Opinion, *He Was Arrested Because of a Computer Error. Now He Wants to Fix the System.*, DETROIT FREE PRESS (June 24, 2020, 6:38 PM), https://www.freep.com/story/opinion/columnists/nancy-kaffer/2020/06/24/robert-williams-detroit-police-facial-recognition/3247171001/ [https://perma.cc/Q3WQ-PDH5]. For those in the industry, however, the case highlighted the impact of poor police work and training. Detectives reported that the surveillance footage did not seem to match the suspect but then used as a comparison a driver's license photo that was no longer a good match for the suspect today. The move from surveillance identification to the use of a dated driver's license introduced dangers of error. There was also the failure to confirm facts beyond the FRT result that would have excluded Williams.

[199] *See* Terry v. Ohio, 392 U.S. 1 (1968). A similar debate arose over the use of body cameras. *See* Floyd v. City of New York, 959 F. Supp. 2d 668, 685 (S.D.N.Y. 2013) (noting that use of body cameras "will provide a contemporaneous, objective record of stops and frisks").

[200] *See supra* note 95 and accompanying text.

[201] David White, Richard I. Kemp, Rob Jenkins, Michael Matheson & A. Mike Burton, *Passport Officers' Errors in Face Matching*, PLOS ONE, Aug. 2014, at 2-6 ("Across all experiments, we found large individual differences on face matching tests, with some people performing with 100% accuracy, and a significant proportion performing quite poorly (below 70% accuracy, on tasks where chance performance is 50%).").

error rate was high with an overall matching rate of only 70%.[202] This was in a controlled environment with both the subjects and good quality photos in front of the officers, as opposed to a street with varying lighting and recollection of a prior image.

The differential in performance can be more inimical to individual rights than a controlled use of biometric technology like FRT.[203] Consider the Boston Marathon Bombing, after which police declared a "containment zone" and forced families into the street with their hands in the air.[204] The suspect, Dzhokhar Tsarnaev, was ultimately found outside the zone once authorities abandoned near-martial law.[205] Once people were "allowed out of their homes and with millions of new eyes on the street, Tsarnaev was quickly spotted hiding in a boat."[206] In such a situation, FRT could help law enforcement avoid time-consuming area searches and the questionable practice of forcing people out of their homes to physically examine them. As Tsarnaev and his brother traveled around Boston, FRT systems might have identified them and ultimately prevented the need for such draconian measures. Conversely, there is the obvious privacy loss associated with a technology that can immediately identify people and track their movements and associations. The specter of a fishbowl society looms over nations that have eagerly embraced FRT, such as China.

These privacy concerns are magnified by the storing of images, which is not related to FRT but instead to the databanks used for the 1:N matches. In assessing the privacy implications, it is important to start with the status of FRT under existing privacy cases and doctrines. As discussed below, FRT and other biometric technology fall into a blind spot under privacy protections. Absent a major (and unlikely) overhaul of controlling precedent, it is not likely that FRT will be curtailed substantially for private or even government use under the Constitution. Three dynamics emerge from privacy case law relevant to FRT and biometric privacy.

A. *The Public Versus Private Dynamic*

If society is going to protect privacy, we need to establish the concrete interests being protected. The most discussed—and most sought after—biometric technology deals with the identification of people from public areas or sources. Such acquisition of facial images, gait, heartbeat, or other

---

[202] *Id.* at 3.

[203] Notably, FRT was originally resisted by CBP but has been accepted because its usage successfully reduced false arrests. Brandi Vincent, *How Facial Recognition Is Changing CBP Operations*, NEXTGOV (July 25, 2019), https://www.nextgov.com/emerging-tech/2019/07/how-facial-recognition-changing-cbp-operations/158704/ [https://perma.cc/VQT9-SRU9].

[204] Jonathan Turley, *A Fishbowl Society Won't Stop Terrorism*, USA TODAY, Apr. 29, 2013, at 8A ("[T]he crisis might have been shortened if the police had not shut down an entire city to look for the suspect by conducting warrantless raids on countless homes . . . .").

[205] *Id.*

[206] *Id.*

information is done without the subject's consent. However, courts have long treated the decision of going out into public as its own consent to be observed. As one court put it, "There can be no privacy in that which is already public."[207] This public/private distinction cuts through privacy jurisprudence as a constitutional Rubicon. This divide was most evident in *California v. Ciraolo*,[208] in which the Court considered privacy protections from aerial surveillance.[209] The Court again declared that "[t]he touchstone of Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'"[210] It then dismissed the notion that such an expectation exists when activities can be observed from a public vantage point, even when the surveillance is coming vertically from the airspace above private property: "The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[211] In *Dow Chemical Co. v. United States*,[212] the Court noted that this was not just because police were in publicly navigable airspace but because "[a]ny person with an airplane and an aerial camera could readily duplicate [these photographs]."[213] Thus, two elements apparently interplay in aerial surveillance cases: First, the observer is in a legal point of observation. Second, anyone—both private individuals and law enforcement—could take such images. Because it makes no sense to deny the images to the police while allowing them for those other than police, the surveillance is constitutional.

The post-*Katz* decisions show how *Katz* itself laid the seeds for the destruction of the privacy protection that Justice Harlan's concurrence purported to protect. While a vast improvement over the archaic trespass doctrine, the Court tied privacy protection to the fluid concept of the "reasonable expectation of privacy."[214] Thus, as technology reduces such expectations, greater surveillance is possible, which reduces those expectations further.[215] This downward spiral can be accelerated in a society saturated by private and governmental surveillance. Moreover, these cases build on each other in declining expectations. Thus, as in *Ciraolo*, the Court's decision in *California v.*

[207] Melvin v. Reid, 297 P. 91, 93 (Cal. Dist. Ct. App. 1931).

[208] 476 U.S. 207 (1986).

[209] *Id.* at 209.

[210] *Id.* at 211 (quoting Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

[211] *Id.* at 213.

[212] 476 U.S. 227 (1986).

[213] *Id.* at 231.

[214] *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

[215] Jonathan Turley, Opinion, *It's Too Easy for the Government to Invade Privacy in Name of Security*, HILL (Nov. 30, 2017, 7:00 AM), https://thehill.com/opinion/judiciary/362500-its-too-easy-for-the-government-to-invade-privacy-in-name-of-security [https://perma.cc/5TD4-5BT3].

Greenwood[216] further reduced privacy expectations when the Court refused to recognize a protected privacy interest in one's garbage.[217] The Court noted that "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[218] The fact that information is "readily accessible" in public would make programs like FindFace particularly transformative, since it is well-known that pictures on the Internet can be used for facial recognition.[219] Placing pictures on the Internet (or even being photographed in public by third parties) could easily be treated as akin to releasing information to a third party. The Court in *Greenwood* found little privacy protection in material that was "placed . . . at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so."[220]

The Court also built on the notion that putting garbage on the curb may constitute implied consent, citing its prior cases stripping away privacy protections in the telephone numbers that are technically given to a third-party telephone company.[221] These cases weigh heavily in favor of allowing the government to use biometric technology like FRT. Not only is this technology readily available to private businesses but also it can acquire images from publicly accessible areas. If current privacy doctrine is left unchanged in the biometric period, the result will be a rapid shift toward a post-privacy existence for many citizens.

B. *The Decisional Versus Informational Dynamic*

Privacy cases have often been divided into cases involving decisional interests and those involving informational privacy interests.[222] The Supreme Court has protected a range of privacy interests for people to make their own decisions on intimacy and personal matters. A wide range of cases falls into this category,

---

[216] 486 U.S. 35 (1988).

[217] *Id.* at 40 (explaining that only expectations of privacy that "society is prepared to accept . . . as objectively reasonable" are afforded Fourth Amendment protection).

[218] *Id.* (footnotes omitted).

[219] *See supra* notes 80-86 and accompanying text (discussing class action over Facebook's facial recognition feature).

[220] *Greenwood*, 486 U.S. at 40.

[221] *Id.* at 41 (citing, inter alia, Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).

[222] *See* Babette Boliek, *Prioritizing Privacy in the Courts and Beyond*, 103 CORNELL L. REV. 1101, 1111-17 (2018); *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 13-26, 188-209 (2004) (describing concerns about rising prevalence of "digital dossiers," collections of detailed data about individuals); Caleb A. Seeley, Note, *Once More unto the Breach: The Constitutional Right to Informational Privacy and the Privacy Act*, 91 N.Y.U. L. REV. 1355, 1359-60, 1359 n.25 (2016) ("In *Whalen v. Roe*, the Court acknowledged that the right to informational privacy is 'implicit in the concept of ordered liberty' and likely protected by the Fourteenth Amendment." (quoting Whalen v. Roe, 429 U.S. 589, 599 n.23 (1977)).

from *Roe v. Wade*[223] to *Griswold v. Connecticut*[224] to *Planned Parenthood of Southeastern Pennsylvania v. Casey*[225] and beyond. Those rulings often treat privacy as a means to protect other rights or interests in procreational choices or personal autonomy. Informational privacy protects the information itself as an extension of Fourth Amendment and tort principles.[226] In *Whalen v. Roe*,[227] the Court itself drew this distinction in noting that cases "sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[228] These divisions, however, tend to lose their definition as courts protect interests like personal autonomy and dignity.[229]

Decisional privacy is far more developed than informational privacy in controlling case law. Indeed, scholarship has struggled to maintain the significance of the division. Some have tried to create a more viable definition of informational privacy by expanding its purpose to political interests and antidiscriminatory policies.[230] FRT and other biometric technology magnify the artificiality—or at least the insufficiency—of the binary division of privacy between decisional and information interests. It is possible to adopt a broader definition of informational privacy to include face prints and biometric data. This will require a substantial revision of the Court's approach to privacy to include digital identity and privacy. Yet, biometric privacy includes both decisional and informational components. Biometric privacy is needed to protect an individual's ability to freely make decisions about their personal and political values. Whether it is the freedom from recognition in places exposing a person's sexual orientation or in the crowd of a political rally, the ability to preserve a degree of anonymity is essential to individual development. In general, biometric privacy is needed to protect information on intimate associations and

[223] 410 U.S. 113, 153-54 (1973) (holding that right of privacy extends to "a woman's decision of whether or not to terminate her pregnancy").

[224] 381 U.S. 479, 485-86 (1965) (finding that Connecticut's statute forbidding contraceptives intruded upon marital privacy in violation of the Constitution).

[225] 505 U.S. 833, 877 (1992) (holding that laws that "unduly burden" a person's decision to have an abortion violate their right of privacy and are thus unconstitutional).

[226] *See* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1089, 1102-06 (2006) (reviewing SOLOVE, *supra* note 222).

[227] 429 U.S. 589 (1977).

[228] *Id.* at 598-600 (footnotes omitted).

[229] *See* Richards, *supra* note 226, at 1093; *see also* Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 161 (2015).

[230] *See* Skinner-Thompson, *supra* note 229, at 175 ("Informational privacy's more nuanced constitutional value is in protecting two categories of information—intimate or political information . . . . [A] categorical approach to informational privacy captures informational privacy's normative value while simultaneously helping to avoid the judicial pitfalls of a dignity and autonomy approach.").

interactions. These interests cross First Amendment, Fourth Amendment, and tort interests, among others.

Continuing to redefine decisional and informational privacy is unlikely to offer the broad foundation needed to fully protect biometric interests. It may be necessary to build on *Whalen*'s acknowledgment that past cases recognized at least two different kinds of interests.[231] The Court may need to formulate a third kind of privacy interest to achieve the type of clarity and coherence needed to sustain a system of both constitutional and statutory protections in the face of groundbreaking technology. While biometric identity touches on core rights within the First and Fourth Amendments, a Biometric Privacy Act can further establish statutory protections and a framework. In that sense, the next step in biometric privacy is much like the prelude to the enactment of Title III—limits and prohibitions on electronic surveillance.[232] The Court first recognized the constitutional foundations for such protections before Congress codified rules to protect those interests.

C. *The Privacy Versus Technology Dynamic*

As previously referenced, there is also a long line of cases running through privacy law that address the enhancement of human surveillance capabilities and how that enhancement plays into privacy protections. One of the most important cases in this area was *Kyllo v. United States*,[233] in which the Court held that the use of thermal imagery devices to scan the outside of a residential home constituted an unreasonable search under the Fourth Amendment.[234] These devices share some of the elements in past cases, emphasizing surveillance from public areas. With thermal imaging technology, police can stand on publicly accessible land and read the heat signature emanating from a house to identify growing operations.[235] That was the case when the Interior Department used such a device to identify Danny Lee Kyllo's home as the likely headquarters of an operation growing marijuana plants.[236] Notably, these devices do not distinguish between lawful or unlawful heat-producing activities. And the technology cannot reveal conversations or identify specific conduct within the home. The U.S. Court of Appeals for the Ninth Circuit upheld the admission of the evidence.[237] The Supreme Court reversed 5-4 with Justice Antonin Scalia writing for the majority and Justice John Paul Stevens writing for the dissent. Justice Scalia emphasized that the technology, while used from public areas,

---

[231] *See Whalen*, 429 U.S. at 599-600 (distinguishing interests in independent decision-making and avoided disclosure of personal information).

[232] *See* Jonathan Turley, Note, United States v. McNulty*: Title III and the Admissibility in Federal Court of Illegally Gathered State Evidence*, 80 NW. U. L. REV. 1714, 1715-16 (1986).

[233] 533 U.S. 27 (2001).

[234] *Id.* at 40.

[235] *See id.* at 30.

[236] *Id.* at 29-30.

[237] *Id.* at 31.

made observations of activities within a home.[238] Accordingly he wrote, "In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[239] He also emphasized that thermal imagery devices were not "in general public use."[240]

Justice Stevens emphasized that the information was acquired from public areas and that the heat signatures were not confined to the house. He noted that neighbors could detect such heat signatures and that

> the notion that heat emissions from the outside of a dwelling are a private matter implicating the protections of the Fourth Amendment (the text of which guarantees the right of people "to be secure *in* their . . . houses" against unreasonable searches and seizures . . .) is not only unprecedented but also quite difficult to take seriously. Heat waves, like aromas that are generated in a kitchen, or in a laboratory or opium den, enter the public domain if and when they leave a building. A subjective expectation that they would remain private is not only implausible but also surely not "one that society is prepared to recognize as 'reasonable.'"[241]

The holding of *Kyllo* does not present a significant limit on biometric devices. First, there is no ostensible penetration of a home with FRT given that the vast majority of facial images are acquired from public areas. Second, these devices are in "general public use."[242] Private businesses, computer companies, telephone companies, and other businesses now use a wide array of biometric technology. Given the narrow drafting of Justice Scalia's opinion and the agreement of the dissenting Justices who were willing to categorically allow thermal imagery, devices using FRT should be able to satisfy a majority of the Court under the logic of *Kyllo*.

The Supreme Court again faced a clash of privacy rights with modern technology in *United States v. Jones*. There, the Court held that the use of a GPS device placed on a vehicle was unconstitutional.[243] In 2004, the D.C. Metropolitan Police Department investigated a nightclub owner and obtained a warrant to place a GPS device on his vehicle within ten days for use only within the District of Columbia.[244] The D.C. police violated the warrant by installing the device after ten days and doing so in Maryland. The twenty-eight days of monitoring were therefore warrantless, and the Supreme Court faced the difficult task of determining how such usage of GPS technology fit into current privacy law. The Court declared the use of the GPS device unconstitutional, though it

---

[238] *Id.* at 34.

[239] *Id.* at 37.

[240] *Id.* at 40.

[241] *Id.* at 43-44 (Stevens, J., dissenting) (first alteration in original) (first quoting U.S. CONST. amend. IV; and then quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

[242] *See id.* at 34 (majority opinion).

[243] United States v. Jones, 565 U.S. 400, 410 (2012).

[244] *Id.* at 402-03.

differed on the rationale. Writing for a five-Justice majority, Justice Scalia relied on the long-thought dead trespass doctrine and its emphasis on property-based privacy.[245] He held that it was the *physical trespass*, triggered by placing the GPS device on the car, that tipped the balance.[246] In his concurrence, Justice Alito was joined by three other Justices who opposed Scalia's "[i]ronic[]" and "unwise" revisal of privacy standards based on "18th-century tort law."[247] Instead, these four Justices would have based the outcome on the expectation of privacy under *Katz* due to the prolonged use of the device to track Jones.[248] Justice Sotomayor also authored a key concurrence that could prove the most relevant to biometrics, despite the fact that no other Justices joined her. Sotomayor voted with Scalia rather than Alito while seeming to agree with Alito's analysis in essential points. Yet, she embraced Scalia's "reaffirmation" of precedent.[249] Notably, Sotomayor emphasized the extensive information that could be gathered from the GPS device as well as the implications of massive data storage of such information. She also noted that this "surreptitious[]" practice could "evade[] the ordinary checks that constrain abusive law enforcement practices."[250] Finally, Sotomayor warned that the "[a]wareness that the government may be watching chills associational and expressive freedoms."[251]

On its face, Justice Scalia's narrow majority opinion struggles to avoid expanding the protections under the expectation of privacy model of *Katz*. By emphasizing trespass, Scalia created a wide opening for FRT and other biometric technologies that operate at a distance without touching the subject or the subject's property. However, Justice Sotomayor's concurrence touched on the underlying fear associated with FRT and other biometric technology and their ability to chill associational or expressive rights. That fear was only mentioned in passing by the majority and falls largely outside of the privacy analysis in both Justice Scalia's and Justice Alito's decisions in *Jones*. Indeed, the interests protected by that chilling effect are not classic privacy interests but are democratic privacy interests that should instead be the focus of the biometric technology analysis. The optimal protections for privacy greatly depend on defining specific interests and explaining why they deserve protection in an environment that is becoming increasingly saturated with biometric technology.

---

[245] *Id.* at 406; *see also* Jonathan Turley, *Are You Being Watched? It's Your Fault.*, WASH. POST, Nov. 13, 2011, at B3.

[246] *Jones*, 565 U.S. at 410.

[247] *Id.* at 418-19 (Alito, J., concurring in the judgment).

[248] *Id.* at 427-28, 430.

[249] *Id.* at 414 (Sotomayor, J., concurring).

[250] *Id.* at 416.

[251] *Id.*

III. ANONYMITY AND DEMOCRACY: A CASE FOR BIOMETRIC PRIVACY AS A CONDITION FOR PARTICIPATORY DEMOCRATIC ACTION

The ubiquitous presence of privacy in both literature and law should suggest that there is a generally accepted definition of this right. Yet, one of the most fascinating aspects of privacy scholarship is the absence of a single accepted definition or understanding of what privacy is or where it comes from. Indeed, Kim Scheppele describes the different uses of the term "privacy" as "an embarrassment of meaning[]."[252] Indeed, privacy is a relatively recent addition to the defined rights under the Constitution, with the first full articulation coming in *Griswold v. Connecticut* in 1965.[253] Some scholars view privacy as an essential element to being human, an inviolate space where individuals may reside or retreat without fear of being monitored or menaced.[254] Others, particularly the courts, tend to treat privacy as a condition or state tied to particular circumstances or property. Under that view, privacy is more epistemic and contextual. Part of the confusion that persists in discussions of privacy is because courts and commentators often use the same word while assigning completely different meanings to it. The fundamental problem of the meaning of "privacy" weighs heavily in the debate over biometric privacy.

A. *The Normative Model*

There has been excellent prior discussion of the opposing concepts of normative versus descriptive privacy rights.[255] Privacy is viewed as an essential component to concepts of personal autonomy and dignity. It is the condition required to fulfill human expression and growth, and it is the protected realm in which intimacy and love can flourish. Many share the view of acting legend Marlon Brando, who once said, "Privacy is not something that I'm merely entitled to[,] . . . it's an absolute prerequisite."[256] Just as humans have a deep pull toward being part of a community, they also need a type of isolation. It is the great paradox of the species: a need for both interaction and seclusion. There is a general view that life in an Orwellian fishbowl society would gradually destroy individuals and make them less human. Louis Brandeis, who, while a Supreme Court Justice, famously described privacy as "the right to be let alone," saw it as an essential human component, heralding the Founders' recognition of "the

---

[252] KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 184-85 (1988); *accord* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 479-80 (2006).

[253] *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

[254] *See generally, e.g.*, Warren & Brandeis, *supra* note 72.

[255] For a discussion of the differences between the normative and descriptive concepts of privacy, see Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, 101 VA. L. REV. 691, 699-702 (2015).

[256] DAVID SHIPMAN, BRANDO: THE MOVIE MAKERS 113 (1974).

significance of man's spiritual nature, of his feelings and of his intellect."[257] Some of Brandeis's writings remain relevant to the type of exposure threatened by FRT and other biometric technology in protecting what Brandeis called the "inviolate personality."[258] While speaking largely of physical privacy, Warren and Brandeis spoke of the implications of being stripped of a protected space: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[259]

Yet, even those who view privacy as key to human development can also view it as a "luxury" of civilization.[260] That was the view expressed by Phyllis McGinley, who referred to privacy as something that has always been the mark of privilege where "those who could afford it chose the luxury of a withdrawing-place."[261] It is undeniable that for much of the history of humankind there was little privacy or expectation of it. Indeed, even through the mid-nineteenth century, most Americans knew few private places other than the vast frontier of open spaces.[262] People lived, loved, and died in single-room structures.[263] Privacy as a moral or normative concept was largely attached to certain objects like letters and keepsakes. At most, there was a moral claim to governance over one's home. The concept of the home being a "man's castle," however, is not a very compelling example of a moral claim to privacy.[264] As discussed below, the protection of the home was couched as a protection from the abuse of governmental power as opposed to the protection of the private matters within.[265]

A review of cases addressing privacy concerns shows that, although courts have recognized the moral or normative claim to privacy, it has rarely been used as a foundation for a right to privacy. Those holding a normative view see

[257] Olmstead v. United States, 277 U.S. 438, 478 (1928). This view was echoed in Brandeis's writings, including his famous law review article with Samuel Warren. *See* Warren & Brandeis, *supra* note 72, at 193, 205.

[258] Warren & Brandeis, *supra* note 72, at 211-12. *See generally* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007) (positing that Samuel Warren, Louis Brandeis, and William Prosser did not create privacy law but instead created new path turning from law of confidentiality).

[259] Warren & Brandeis, *supra* note 72, at 195.

[260] This point is raised by figures like William Manchester who wrote of "the medieval man's total lack of ego. Even those with creative powers had no sense of self." WILLIAM MANCHESTER, A WORLD LIT ONLY BY FIRE: THE MEDIEVAL MIND AND THE RENAISSANCE PORTRAIT OF AN AGE 21 (1st paperback ed. 1993).

[261] PHYLLIS MCGINLEY, THE PROVINCE OF THE HEART 56 (1959).

[262] *See id.*

[263] *Id.*

[264] *See* WILLIAM BLACKSTONE, 3 COMMENTARIES ON THE LAWS OF ENGLAND: OF PRIVATE WRONGS 288 (1768).

[265] *See infra* Section III.B.

privacy as a necessity of human growth and happiness. Yet, humans did not know—let alone enjoy—it for thousands of years. Moreover, the recognition of a right to privacy on moral grounds does not answer the question of most cases for the courts. There are any number of rights that are normatively based in free speech and free exercise. However, none is absolute and each must be balanced against the countervailing interests of the government or opposing party. For those reasons, the more abstract justification for privacy may have been referenced in decisions but rarely served as the determinative basis for a prevailing party. For example, it is notable that cases like *Karo* find an injury in the act of tracking a citizen inside their home.[266] The threat was to the disclosure of generally described private information, or information "that could not have been visually verified."[267] In the same way, the Court in *Kyllo* noted that, when looking at the home, "*all* details are intimate details, because the entire area is held safe from prying government eyes" and that penetration into this private setting is sufficient to warrant Fourth Amendment protections.[268]

Under the common law, the normative view of privacy is captured in the intrusion upon seclusion tort.[269] Courts have overwhelmingly rejected claims of intrusion for conduct occurring in public, but there are exceptions. In *Nader v. General Motors Corp.*,[270] for example, consumer activist Ralph Nader was followed and harassed by private detectives hired by GM after his breakthrough 1965 publication of *Unsafe at Any Speed* exposed the dangerous conditions of American automobiles.[271] The Court of Appeals of New York rejected most of the claims that Nader brought against the detectives but found that when the detectives looked over Nader's shoulder while he was filling out a bank slip, they had intruded upon his seclusion. The court noted that

> the mere observation of the plaintiff in a public place does not amount to an invasion of his privacy. But, under certain circumstances, surveillance may be so "overzealous" as to render it actionable. . . . A person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing.[272]

A couple of important distinctions should, however, be noted about *Nader*. First, not only is addressing privacy fairly unique among torts cases but also the court was addressing Nader's privacy in the bank while performing a private

[266] *See* United States v. Karo, 468 U.S. 705, 730 (1984).

[267] *Id.* at 715.

[268] Kyllo v. United States, 533 U.S. 27, 37 (2001).

[269] RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

[270] 255 N.E.2d 765 (N.Y. 1970).

[271] *Id.* at 767.

[272] *Id.* at 771.

function. It was not claiming that his movements were in any way protected. Moreover, in a statement with obvious relevance to biometric controversies, the court stressed, "It should be emphasized that the mere gathering of information about a particular individual does not give rise to a cause of action under this theory. Privacy is invaded only if the information sought is of a confidential nature and the defendant's conduct was unreasonably intrusive."[273]

Biometric technology raises issues of personal autonomy when it is applied to biometric material taken without consent. However, FRT is designed to use public information or images. Indeed, many images can be "mined" from voluntary disclosures made on social media and the Internet. Much like the implied consent that is attendant to walking out into public, the same implied consent is found in voluntarily putting one's images on the Internet. That moves most technology outside of the type of analysis used in reproductive or intimacy cases. Indeed, even on issues of intimate relations and marriage, the Supreme Court developed a separate line of cases based on the right to "dignity" as opposed to privacy or equal protection.[274]

While various scholars have argued for what Helen Nissenbaum has called "privacy in public,"[275] the courts continue to maintain the strong situational divide of public versus private conduct. This view is magnified when placed into the dichotomy of citizen versus government interests. Courts tend to view the constitutional protections under the Fourth Amendment as functional and limited, rather than normative. Due to the use of biometrics in observable public settings, the normative model offers an insufficient foundation for biometric privacy claims.

B. *The Criminal Justice Model*

The concept of an enforceable right to privacy arose in tandem with the government's criminal investigative powers. As the government asserted greater police powers, privacy concerns arose regarding the demarcation of authority between the individual and the state. For that reason, privacy was forged first and foremost in the context of the criminal justice system. Indeed, since Roman times, individuals have claimed that the home constituted a protected area as distinct from searches on the road or in public.[276] Obviously, however, this was not an absolute protection against the government. It affirmed the right to resist others who would invade or disturb a home.[277] This was put in almost Hobbesian terms by John Adams in his arguments in the case *King v. Stewart*. Richard King

---

[273] *Id.* at 769; *accord* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

[274] *See, e.g.*, United States v. Windsor, 570 U.S. 744, 775 (2013).

[275] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT 113-26 (2010) (discussing private/public sphere dichotomy as a possible cutoff for privacy claims).

[276] *See* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 15-18 (1937).

[277] *See id.* at 16 (discussing procedure in courts for victim of theft to obtain "warrant" to gather evidence from accused's home).

was the subject of a mob attack in which his home and store were invaded and burned.[278] In his inimical style, Adams declared that such an invasion was a denial of the basic sovereignty of every person over the home:

> An Englishmans [sic] dwelling House is his Castle. The Law has erected a Fortification round it—and as every Man is Party to the Law, i.e. the Law is a Covenant of every Member of society with every other Member, therefore every Member of Society has entered into a solemn Covenant with every other that he shall enjoy in his own dwelling House as compleat a security, safety and Peace and Tranquility as if it was surrounded with Walls of Brass, with Ramparts and Palisadoes and defended with a Garrison and Artillery.[279]

Notably, this oft-quoted argument was directed against other individuals, not the government. Nevertheless, the "castle" concept also embodied a notion that the home was a protected space from casual or arbitrary searches, a principle that was ultimately affirmed in the Fourth Amendment's protection against "persons, houses, papers and effects, against unreasonable searches and seizures."[280]

The Fourth Amendment's language is itself revealing in two important respects. First, it is only a protection against the government. If privacy was viewed as an overarching moral prerogative, one would expect a broader affirmation of this right outside of the criminal justice system. Second, it is not articulated in terms of the privacy right itself but in terms of the specific contexts where individuals are afforded protection from search or seizure, and even those areas of protection could be lost to a warrant with a simple showing of probable cause. Courts have spent decades exploring that line of demarcation but rarely alluded to a greater moral justification for privacy. Indeed, the most famous defense of privacy by the Supreme Court was closely tied to the criminal justice system. In *Olmstead*, Justice Brandeis penned his famous dissent in which he declared, "The makers of our Constitution . . . conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[281] Brandeis's "right to be let alone," however, was actually a right to be left alone by the government, given that the

---

[278] JOHN ADAMS, *Writ of Review*—Stewart et. al. v. King, *in* 1 LEGAL PAPERS OF JOHN ADAMS 113, 113-16 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965).

[279] JOHN ADAMS, *Argument and Report*, *in* 1 LEGAL PAPERS OF JOHN ADAMS, *supra* note 278, at 132, 137.

[280] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[281] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

majority ruled that there was no Fourth Amendment violation if the *government* did not engage in an actual trespass in order to carry out the surveillance.[282]

These Fourth Amendment expectation of privacy cases draw heavily on the public/private distinction. Once a citizen steps outside, the protections that are afforded to them while in their home largely evaporate. By venturing into public, one has elected not to be alone. Thus, in cases like *Knotts*, the Court has dismissed the idea of an expectation of privacy in not being tracked by a device placed in one's car because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[283] Of course, one could argue that a person can have an expectation of privacy even if they are capable of being seen.

My colleague, Daniel Solove, has described the "secrecy paradigm" running in these cases as the notion that disclosed information is no longer a secret and thus disclosed to the world.[284] He noted that this paradigm forces information to be "categorized as either public or private. . . . Understood this way, information has a particular status; it can either be in one domain or another. The law often treats information in this black-and-white manner; either it is wholly private or wholly public."[285] Yet, Solove points out that we do many things in public that we assume are relatively shielded, such as have whispered conversations or make discrete purchases.[286] Nevertheless, Solove concludes that the "secrecy paradigm" is still largely adhered to in the Supreme Court's Fourth Amendment jurisprudence.[287]

Because of the criminal justice model's predominant assumption in favor of formalistic privacy distinctions, it is unlikely to serve as effective protection from emerging biometric technology. As shown above, most of the privacy cases dealing with public spaces and technological enhancement are largely within the criminal justice realm. These cases offer little insight or assistance in dealing with a threat that is metastasizing through the expansion of consumer products that utilize the same transparency-forcing technology.

---

[282] Even Justice Brandeis spoke of privacy as a protection against the disclosure of information by another means. He noted that protections are needed to combat "[s]ubtler and more far-reaching means of invading privacy [that] have become available to the Government . . . by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." *Id.* at 473.

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

[284] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1176 (2002).

[285] *Id.* at 1177.

[286] *See id.* at 1178 (describing how people know that some things done publicly will be shielded from public access because they "will be lost in a sea of information about millions of people").

[287] *Id.* at 1184.

C. *A Democratic Model*

In 1980, Professor Ruth Gavison wrote powerfully for the articulation of a freestanding right of privacy, finding such a right essential for protecting underlying interests of individuals in their personal and informational privacy.[288] Absent such a clear definition and recognition, those ethereal interests would slowly lose ground in the balancing act between the more concrete interests of the government and society.[289]

In cases like *Russell v. Gregoire*,[290] litigants have argued that "the accumulation and dissemination of information about them violate[d] their right to privacy."[291] However, in *Russell* the Ninth Circuit declared the argument "fatally defective" because the litigants could "not pinpoint the source of the right or identify its contours."[292] Courts have grappled with finding the constitutional basis for protecting informational privacy due to this lack of definition and have left protections largely to legislative initiatives.[293] Now, four decades later, society is in a similar position with biometric privacy. There is a growing need to articulate the right of anonymity in modern society if that interest is to have any serious weight in the balancing of society's interests. If viewed entirely from the traditional privacy perspective, biometrics are likely to be dangerously untethered from constitutional restraints and protections from biometric identification will derive entirely from statutory or regulatory action. From an expectation of privacy perspective, the public acquisition of images largely negates constitutional limits.[294] A desire to protect public movements comes across as an argument for "privacy in public," and similar claims have long been rejected by courts.[295] From a trespass or privacy perspective, there is no need to physically touch—let alone trespass—on personal property for biometrics to gain information. After the Supreme Court famously declared that

---

[288] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 424 (1980).

[289] *See id.* at 458 (describing how "[t]he limits of law in protecting privacy stem . . . from the law's commitment to interests that sometimes *require* losses of privacy").

[290] 124 F.3d 1079 (9th Cir. 1997).

[291] *Id.* at 1093 (rejecting challenge to state sex offender notification statute); *see also* Skinner-Thompson, *supra* note 229, at 164-65 (describing how courts have been challenged to clearly articulate the right to privacy and to identify its many values).

[292] *Russell*, 124 F.3d at 1093.

[293] *See generally* Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 1–1 (Ryan P. Blaney ed., 2d ed. 2020).

[294] *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 101 (2011) ("The secrecy paradigm has resulted in many forms of government information gathering falling outside Fourth Amendment protection. This is a big problem, because when the Fourth Amendment doesn't apply, there's often nothing to regulate the government.").

[295] Samantha Barbas, *Saving Privacy from History*, 61 DEPAUL L. REV. 973, 991 (2012).

the Fourth Amendment "protects people, not places,"[296] one category of "places" remains largely unprotected under privacy jurisprudence—public places.[297] Thus, the effort to attach protections to the person (based on an expectation of privacy) still collapses when that person ventures out of a protected place. Yet, public places are where key political activities and associations occur, from door-to-door solicitations to rallies to pamphleteering.

In his 1978 foundational article, Professor Frederick Schauer discussed claims of potential chilling effects of government surveillance and rejected the viability of such claims because they cannot rest on "specific, and most likely unprovable, predictions of human behavior."[298] The Supreme Court shared this skepticism in its early discussion of chilling effects from government surveillance. In *Laird v. Tatum*,[299] the Court held that the chilling effect of the Army's surveillance of civilian political activities was an insufficient injury-in-fact to allow the plaintiffs standing to challenge the program.[300] The Court dismissed what it referred to as "less generalized yet speculative apprehensiveness" about the impact of such surveillance on political associations and speech.[301] It held that "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[302]

Despite this initial skepticism, the Court has often raised governmental or privacy conduct's chilling effect on core constitutional functions.[303] One such example was the decision in *New York Times Co. v. Sullivan*,[304] in which the Court limited defamation actions against the media to protect the key role of a

[296] Katz v. United States, 389 U.S. 347, 351 (1967).

[297] *Id.*

[298] Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 730-31 (1978); *see also* Jessica A. Clarke, *Explicit Bias*, 113 NW. U. L. REV. 505, 573-74 (2018) (noting that "chilling effects arguments are more fundamentally about a normative question: whether the law should favor the risk averse who will over-comply with legal restrictions and err on the side of protecting free speech" as opposed to accepting that the relevant government interest can only be safeguarded by limiting free speech); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 155 (2007) [hereinafter Solove, *The First Amendment as Criminal Procedure*] ("Determining the existence of a chilling effect is complicated by the difficulty of defining and identifying deterrence. It is hard to measure the deterrence caused by a chilling effect because it is impossible to determine with certainty what people would have said or done in the absence of the government activity.").

[299] 408 U.S. 1 (1972).

[300] *Id.* at 13.

[301] *Id.* at 13-14.

[302] *Id.*

[303] *See* Solove, *The First Amendment as Criminal Procedure*, *supra* note 298, at 142-59.

[304] 376 U.S. 254 (1964).

free press in our constitutional system.[305] The underlying lawsuit was one of a litany of strategic defamation actions that were intended to bleed the media covering the civil rights movement. As with the early surveillance cases, there had been a long line of cases leaving such defamation actions to the states and rejecting protection from defamation actions under the First Amendment.[306] However, the Court came to recognize that this previously unprotected area of speech creates a threat to the robust and uninhibited exchange of ideas in society. In his opinion for a unanimous Court in *New York Times*, Justice Brennan wrote that the Constitution demanded "breathing space" for the type of "uninhibited, robust, and wide-open" speech needed to sustain a free nation, particularly on political issues.[307] The Court cited the danger of losing "the vigor and . . . the variety of public debate" that is needed in a democratic system.[308] The Court believed that common-law torts were discouraging media from performing its essential functions under the First Amendment.[309] Accordingly, the Court created a higher standard for public officials to satisfy in suing critics or journalists for defamation.[310] The Court's action to bar the common law from "encroach[ing] on freedom of utterance"[311] reflects how the Court protects the necessary "breathing space" under the First Amendment.[312] Unrestrained use of FRT and other biometric technology threatens the same "breathing space" needed for free speech and privacy rights by eliminating the anonymity that is essential for allowing people to freely encounter and associate with different causes.

[305] *Id.* at 291-92 (limiting defamation actions against the media for false statements about public officials because holding otherwise would raise "the possibility that a good-faith critic of government will be penalized for his criticism," which "strikes at the very center of the constitutionally protected area of free expression").

[306] *See, e.g.*, Beauharnais v. Illinois, 343 U.S. 250, 266 (1952). Through these cases, the Court maintained that defamatory statements played "no essential part of any exposition of ideas." Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).

[307] *New York Times*, 376 U.S. at 270-72.

[308] *Id.* at 279.

[309] *Id.* at 292.

[310] *Id.* at 279-80. Notably, three Justices wanted to go further and simply ban such actions. *Id.* at 297 (Black, J., joined by Douglas, J., concurring) ("This Nation, I suspect, can live in peace without libel suits based on public discussions of public affairs and public officials. But I doubt that a country can live in freedom where its people can be made to suffer physically or financially for criticizing their government, its actions, or its officials."); *id.* at 298 (Goldberg, J., joined by Douglas, J., concurring in the result) ("In my view, the First and Fourteenth Amendments to the Constitution afford to the citizen and to the press an absolute, unconditional privilege to criticize official conduct despite the harm which may flow from excesses and abuses.").

[311] *Id.* at 268 (majority opinion) (quoting Beauharnais v. Illinois, 343 U.S. 250, 263-64 (1952)).

[312] *Id.* at 272 (quoting NAACP v. Button, 371 U.S. 415, 433 (1963)).

1. Anonymity and Observation in Human Conduct

A recognition of the central importance of anonymity is missing. In *The Spirit of Laws*, Montesquieu famously declared that "we must consider man before the establishment of society."[313] The importance of anonymity to the democratic process rests heavily on the impact of anonymity on human conduct.[314] It has long been understood that observation—or the possibility of observation—affects human behavior and conduct. The impact of observation on human behavior is often called "the Hawthorne Effect," named after an experiment at the Hawthorne factory in Chicago in 1924.[315] That effect can produce a socially positive result. Thus, there is a trend in favor of body cameras for police officers not just to record arrests but also to reduce the likelihood of abusive behavior by or toward the police. Studies have shown that such observation cut use of force incidents by 50% and cause similar drops in citizen complaints.[316]

Even the subtlest changes in conduct can have a profound impact on social discourse and associations. For years, I have taught the fragility of privacy

[313] MONTESQUIEU, THE SPIRIT OF LAWS 20 (Thomas Nugent trans., Batoche Books 2001) (1748).

[314] Ruth Gavison identified three components in defining privacy, "secrecy, anonymity, and solitude." Gavison, *supra* note 288, at 433.

[315] *See* Stephen R.G. Jones, *Was There a Hawthorne Effect?*, 98 AM. J. SOC. 451, 451 (1992) ("[T]he central idea [of the Hawthorne effect] is that behavior during the course of an experiment can be altered by a subject's awareness of participating in the experiment."); C.E. Snow, *Research on Industrial Illumination: A Discussion of the Relation of Illumination Intensity to Productive Efficiency*, 8 TECH ENGINEERING NEWS 257, 257 (1927) (describing how increased illumination led to increase in production rate of employees); *see also* Steven D. Levitt & John A. List, *Was There Really a Hawthorne Effect at the Hawthorne Plant? An Analysis of the Original Illumination Experiments*, AM. ECON. J.: APPLIED ECON., Jan. 2011, at 224, 229-36 (performing statistical analysis of original Hawthorne data). While the methodology of the Hawthorne study and interpretation of its effect has been questioned, other studies have found that this effect does in fact exist. *Compare, e.g.*, John G. Adair, *The Hawthorne Effect: A Reconsideration of the Methodological Artifact*, 69 J. APPLIED PSYCHOL. 334, 337 (1984) (describing how psychology textbooks misinterpret the Hawthorne studies and noting that the studies contained "so many uncontrolled variables that it became virtually impossible to identify any causative relationships," which likely led to confusion), *with* Jim McCambridge, John Witton & Diana R. Elbourne, *Systematic Review of the Hawthorne Effect: New Concepts Are Needed to Study Research Participation Effects*, 67 J. CLINICAL EPIDEMIOLOGY 267, 274 (2014) (reviewing nineteen studies on Hawthorne Effect and reporting that twelve studies "provided at least some evidence of the existence of a Hawthorne effect").

[316] *See generally* LEE RANKIN & TONY FILLER, MESA POLICE DEP'T, END OF PROGRAM EVALUATION & RECOMMENDATIONS: ON-OFFICER BODY CAMERA SYSTEM 1 (2013); Wesley G. Jennings, Matthew D. Lynch & Lorie A. Fridell, *Evaluating the Impact of Police Officer Body-Worn Cameras (BWCs) on Response-to-Resistance and Serious External Complaints: Evidence from the Orlando Police Department (OPD) Experience Utilizing a Randomized Controlled Experiment*, 43 J. CRIM. JUST. 480, 482-84 (2015) (finding that body-worn cameras reduced use of force incidents by 53.4% and external complaints by 65.4%).

interests with a simple assignment for my students. During holiday break, I ask them to bring a small tape recorder with them. At small informal gatherings like breakfast with family or drinks at a bar with friends, they had to put the recorder on the table and explain that they are just going to record their conversations for a class. The recorder was empty, but they would pretend to turn it on and assure their friends that no one but the student would listen to it. I asked them to note how conversation would immediately change on subject matter and language. Suddenly, their friends would often stop trash-talking and begin to speak in complete sentences. Some might view such changes as positive. Certainly, countries such as China believe that surveillance will instill better citizen conduct. However, the changes are so subtle that many speakers may not realize that they changed the way they are relating to their closest friends. Even the possibility of observation or recording alters the range of what is considered permissible or advisable in conversation or conduct.

Studies demonstrate a type of digital Hawthorne effect from the fear of surveillance.[317] A study by Elizabeth Stoycheff examined changes in postings to Facebook after the disclosure of PRISM, a secret online surveillance program led by the U.S. National Security Agency ("NSA") in 2013.[318] Stoycheff found a pronounced change in views and association on Facebook following the disclosure of the NSA/PRISM program: "[W]hen these individuals perceive they are being monitored, they readily conform their behavior—expressing opinions when they are in the majority, and suppressing them when they're not."[319] A similar study on changes in postings on Wikipedia found that the public disclosure of the NSA/PRISM program "caused the sudden drop during and after June 2013, as well as the general trend reversal, for the terrorism-related Wikipedia articles."[320] People felt chilled in even creating a record of inquiry about these subjects—evidenced by a 19.5% drop in traffic on the monitored stories.[321]

It is also true that anonymity can have negative consequences on human behavior. The famous Stanford experiments of Philip Zimbardo in 1969 showed how anonymity can release individuals from a sense of obligation or even

[317] Privacy groups have cited these studies have when seeking judicial review of the programs under existing privacy case law with limited success. *See, e.g.*, Karen Gullo, *Surveillance Chills Speech—as New Studies Show—and Free Association Suffers*, ELECTRONIC FRONTIER FOUND. (May 19, 2016), https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association [https://perma.cc/7EK8-4EKN].

[318] Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. Q. 296, 307 (2016).

[319] *Id.* at 307.

[320] Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 161 (2016).

[321] *Id.* at 146.

humanity.[322] In Zimbardo's experiment, some students were anonymous and given hoods while others were hoodless and given name tags.[323] The anonymous students electrically shocked their fellow students for twice as long as the students with name tags.[324] Other studies have found that anonymity and group dynamics could lead to similar socially dysfunctional conduct such as calling for suicidal individuals to jump from buildings.[325] Anyone who browses the Internet can see the negative aspects of anonymity as people unleash racist, anti-Semitic, and other hateful thoughts under the protection of assumed identities.[326]

Yet, all rights carry the danger of abuse. For example, we accept a great deal of "bad speech" to foster "good speech." Indeed, the greatest weapon against hate speech is not censorship but corrective speech from others.[327] While white nationalists and groups like Antifa may use masks to hide identities during violent protests, there are many more protesters who carry out nonviolent and beneficial demonstrations as part of the political system.[328] Those associations and activities drive reforms in the political system as these rights quickly become anemic and diminished under governmental regulation. The Supreme Court has often warns about the chilling effects of government actions as the "collateral effect of inhibiting the freedom of expression, by making the individual the more reluctant to exercise it."[329] Thus, in *Miami Herald Publishing Co. v. Tornillo*,[330] the Court unanimously struck down a statute that required newspapers to publish a reply from any political candidate criticized by that newspaper.[331] Such a law clearly presented an inhibiting influence on editors writing their columns on

[322] Philip G. Zimbardo, *The Human Choice: Individuation, Reason, and Order Versus Deindividuation, Impulse, and Chaos*, 17 NEB. SYMP. ON MOTIVATION 237, 268 (1969).

[323] *Id.* at 264.

[324] *Id.* at 269-70.

[325] *See* Leon Mann, *The Baiting Crowd in Episodes of Threatened Suicide*, 41 J. PERSONALITY & SOC. PSYCHOL. 703, 703 (1981).

[326] *See* Christopher P. Barlett, Douglas A. Gentile & Chelsea Chew, *Predicting Cyberbullying from Anonymity*, 5 PSYCHOL. POPULAR MEDIA CULTURE 171, 177 (2016) (finding that "the more people feel that they are anonymous online, the more likely they are to cyberbully others"); Kimberly M. Christopherson, *The Positive and Negative Implications of Anonymity in Internet Social Interactions: "On the Internet, Nobody Knows You're a Dog,"* 23 COMPUTERS HUM. BEHAV. 3038, 3050 (2007) (outlining theories of effects of anonymity in computer-mediated communications).

[327] *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[T]he best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.").

[328] *The Right of the People Peaceably To Assemble: Protecting Speech by Stopping Anarchist Violence: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 116th Cong. (Aug. 4, 2020) (written testimony of Professor Jonathan Turley) (on file with author).

[329] *See, e.g.*, Smith v. California, 361 U.S. 147, 151 (1959).

[330] 418 U.S. 241 (1974).

[331] *Id.* at 258.

matters of public importance. The Court noted that "[g]overnmental restraint on publishing need not fall into familiar or traditional patterns to be subject to constitutional limitations on governmental powers."[332] Yet, the chilling effects are felt in a variety of protected actions. For the purposes of FRT and other biometric technology, the interests that should be protected fall in a convergent area between speech and privacy.

These interests are not tied to a normative theory but to a descriptive one. Descriptive privacy models keenly note the specific values that privacy protects. Privacy can be treated as essential to one's dignity or autonomy interests. Privacy is not a normative value in itself but a condition needed to sustain other values. Biometric privacy is best understood in such a descriptive fashion. As a normative matter, protecting public information does not sit well with past normative arguments. Likewise, given the case law surrounding public spaces, the concern about a fishbowl society does not actually prove determinative in cases. Even the GPS and thermal imagery cases were narrowly construed and will not present serious barriers to the use of FRT or other biometric technology.[333] Yet, the Supreme Court is rightfully wary of the chilling effects that privacy threats can pose towards speech and other interests. The Court has also protected rights like anonymity based on broader grounds related to the democratic process and to political expression. This alternative view captures the most concerning aspect of biometrics—its ability to disrupt personal and political expression. Indeed, this is precisely why biometrics, and especially FRT, captivate authoritarian regimes.

2. Anonymity as a Protected Right

As discussed in Section III.C.1, FRT falls into a blind spot of constitutional doctrines. Rights of free speech, association, and privacy have at times been defined in insular or narrow ways. Alternatively, they can be connected in a functional way to broader roles within the democratic process—protected not simply because of their normative value but because of their vital function in protection of political processes and expression.[334] Alexander Meiklejohn made this connection between free speech and the democratic process in his work, *Free Speech and Its Relation to Self-Government*.[335] The Supreme Court had

[332] *Id.* at 256.

[333] *See supra* Section II.C.

[334] *See* Kusper v. Pontikes, 414 U.S. 51, 56-57 (1973) ("There can no longer be any doubt that freedom to associate with others for the common advancement of political beliefs and ideas is . . . protected by the First and Fourteenth Amendments."); *see also* Bates v. City of Little Rock, 361 U.S. 516, 523 (1960) ("[I]t is now beyond dispute that freedom of association for the purpose of advancing ideas and airing grievances is protected by the Due Process Clause of the Fourteenth Amendment . . . .").

[335] ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT 24-27 (Kennikat Press 1972) (1948) (arguing that the purpose of the First Amendment is to allow

focused on the threat of speech when it crafted the "clear and present danger" test but failed to broaden its jurisprudence to protect speech because of its functional importance.[336] Meiklejohn sought to make the case for the defense of speech, though he distinguished between public speech and nonpublic speech in terms of such protection. Rather than adopting the Court's focus on defining "dangerous" speech, he focused on what speech was dangerous to limit or suppress: "[O]ur civil liberties, in general, are not all of one kind. They are of two kinds which, though radically different in constitutional status, are easily confused. . . . One of these is open to restriction by the government. The other is not open to such restriction."[337] This bifurcated view of free speech is not popular with scholars who hold more absolutist interpretations. However, Meiklejohn's theory tied the level of protection to the role of speech in a democratic system.

Meiklejohn, and later John Hart Ely,[338] articulated the values that would take hold as the political process model for free speech protections. They defined the scope of this right as an essential part of the protection that the democratic political process has in order to stop majoritarian controls and abuse.[339] Associational rights and privacy further support that same functional political process purpose. One element, however, cuts across all of the rights, from speech to association to privacy: anonymity. Anonymity is also the element of free society most threatened by FRT and other biometric technology. Hence, anonymity should be the focus of efforts to regulate this emerging technology.

Anonymity has always been the bane of tyranny. For an authoritarian government to control its citizens, the government must curtail citizens' conduct, not by unwieldy direct force but through coercion or threat. That control cannot be established if citizens can move, associate, and advocate without fear of retaliation. Retaliation depends on recognition. Biometric technology is the solution to the recognition challenges that authoritarian governments face. The Court often discusses anonymity in speech and privacy cases in descriptive terms. Some of these cases touch on the importance of anonymity to democratic functions, particularly speech. Thus, the Court has recognized that "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association,

free airing of ideas central to self-government rather than to allow "unregulated talkativeness").

[336] Schenck v. United States, 249 U.S. 47, 52 (1919) (holding that First Amendment does not protect speech that "create[s] a clear and present danger that . . . bring[s] about the substantive evils that Congress has a right to prevent").

[337] MEIKLEJOHN, *supra* note 335, at 1-2.

[338] *See* JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW 105-16 (1980) (evaluating standards of judicial review for free speech claims while noting that First Amendment's central function is "assuring an open political dialogue and process").

[339] *Id.*; MEIKLEJOHN, *supra* note 335, at 24-27.

particularly where a group espouses dissident beliefs."[340] Yet, anonymity has always held an uncertain value from the earliest cases.

In 1913, in *Lewis Publishing Co. v. Morgan*,[341] the Court gave short shrift to free press values in upholding a federal law forcing newspapers to give the government a list of any editorial and business officers as a condition for mailing privileges.[342] The Court did not delve into the implications of such reporting on the function of the press or how such conditions might impact the key role of the free press in our democratic system. The same is true for the Court's ruling in *New York ex rel. Bryant v. Zimmerman*,[343] in which the Court upheld a state law requiring the registration of organizations with twenty or more members and for which an oath was required as a condition for membership.[344] The defendant was a member of the KKK, which has long been a hateful organization based on secrecy, illustrated by the wearing of hoods. Yet, the Court again upheld the law with no substantive analysis of how the loss of anonymity might impact the exercise of free speech or association.[345]

The Court's view of anonymity changed by 1958, when the target of such identification of members was the NAACP. In *NAACP v. Alabama ex rel. Patterson*,[346] the Court overturned the Alabama Supreme Court and ruled that the state's requirement of membership lists was a violation of the First Amendment right of association.[347] In sharp contrast to the treatment of the individuals seeking to conceal their membership in the KKK, the Court held that the law had to be evaluated for its impact on constitutionally protected conduct and associations:

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association [as a direct government restriction]. . . . This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. . . . Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[348]

The Court recognized that identification or association with particular groups can

[340] NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958).

[341] 229 U.S. 288 (1913).

[342] *Id.* at 316.

[343] 278 U.S. 63 (1928).

[344] *Id.* at 71-77.

[345] *Id.* at 76-77.

[346] 357 U.S. 449 (1958).

[347] *Id.* at 466.

[348] *Id.* at 462.

> affect adversely the ability of [the NAACP] and its members to pursue their collective effort to foster beliefs . . . [and] may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.[349]

The case includes one line that has particular resonance with FRT. In evaluating the impact on constitutionally protected activities, the Court noted that "[t]he crucial factor is the interplay of governmental and private action."[350] As discussed above, both private and governmental parties use FRT extensively.

In another NAACP case involving compelled membership listing, *Bates v. City of Little Rock*,[351] the Court built further on its prior analysis by stressing that "[f]reedoms . . . are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference."[352] The Court noted that many individuals withdrew from association with the group or declined to join not just because of the disclosure of their names but because of the threat that they could be identified by the government: "This repressive effect, while in part the result of private attitudes and pressures, was brought to bear only after the exercise of governmental power had threatened to force disclosure of the members' names."[353]

These cases are notable not only in their recognition of anonymity but also for their methodological shift toward analyzing the impact of governmental action on the behavior of citizens engaged in expressive conduct. The same year as *Bates*, the Court made a significant step forward in articulating the constitutional significance of anonymity in its ruling in *Talley v. California*,[354] which struck down a Los Angeles ordinance that barred the distribution of anonymous pamphlets supporting a boycott.[355] The Court broadened its analysis to explore how the anonymity of citizens allowed for expressive conduct.

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. The obnoxious press licensing law of England, which was also enforced on the Colonies was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to

[349] *Id.* at 462-63.

[350] *Id.* at 463.

[351] 361 U.S. 516 (1960).

[352] *Id.* at 523.

[353] *Id.* at 524.

[354] 362 U.S. 60 (1960).

[355] *Id.* at 64; *see also* Solove, *The First Amendment as Criminal Procedure*, *supra* note 298, at 145.

> which government had to go to find out who was responsible for books that were obnoxious . . . .[356]

Noting its rulings in earlier cases involving the NAACP, the Court declared that it had recognized that there are "times and circumstances when States may not compel members of groups engaged in the dissemination of ideas to be publicly identified."[357] While FRT is not a registration or listing system, it is a process for public identification that results from any venture into public areas. Such public identification would effectively undermine the holdings of these cases by providing the government with an alternative to compelling citizens in associations to self-identify.

The Court expanded on this line of cases in *McIntyre v. Ohio Elections Commission*,[358] in which the Court invalidated an Ohio statute that barred the distribution of anonymous campaign literature on any political campaign or issue.[359] When Margaret McIntyre passed out leaflets opposing a referendum at a school board meeting, she was sanctioned under state law and fined $100.[360] With Justice Stevens writing for a 7-2 majority, the Court overturned the Ohio Supreme Court's decision and declared the law unconstitutional under the First Amendment.[361] Notably, the Ohio Supreme Court upheld the law on the basis that any "burdens imposed on the First Amendment rights of voters [were] '*reasonable*' and '*nondiscriminatory*.'"[362] That was not sufficient justification for the Supreme Court, however, given the impact of the law on the exercise of First Amendment rights.[363] After discussing the role of anonymity in great literary works, the Court discussed how essential anonymity can be to the preservation of democratic rights. Noting that the Ohio law dealt directly with political speech, the Court stressed that such speech "occupies the core of the protection afforded by the First Amendment."[364] While FRT is not necessarily directed at the type of political activity protected in *McIntyre*, it nevertheless requires constant identification of all public conduct and associations. However, the Court went on to declare that Ohio was purportedly fighting potentially fraudulent speech with a "blunderbuss approach" that swept too broadly.[365] The Court reasoned,

---

[356] *Talley*, 362 U.S. at 64-65.

[357] *Id.* at 65.

[358] 514 U.S. 334 (1995).

[359] *Id.* at 357.

[360] *Id.* at 337-38.

[361] *Id.* at 357.

[362] *Id.* at 340.

[363] *Id.* at 342 ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.").

[364] *Id.* at 346.

[365] *Id.* at 357.

> Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.[366]

Of course, *McIntyre* was not unanimous, and Justice Scalia's objections to the decision would enshrine anonymity as a constitutional right. In his dissent, Justice Scalia posited that anonymity was not a motivating value or right under the original meaning of the Constitution. In his view, "constitutional adjudication necessarily involves not just history but judgment: judgment as to whether the government action under challenge is consonant with the concept of the protected freedom (in this case, the freedom of speech and of the press) that existed when the constitutional protection was accorded."[367] The basis for Justice Scalia's viewpoint seems shaky given that many of the early debates surrounding the First Amendment stemmed from Framers writing anonymously and that the Federalist Papers themselves are a testament to the importance of anonymity.[368] Indeed, it is worth noting that Thomas Paine's *Common Sense* was initially published by an author who identified himself only as "An Englishman."[369] In his concurrence in *McIntyre*, Justice Thomas made that very point:

> There is little doubt that the Framers engaged in anonymous political writing. The essays in the Federalist Papers, published under the pseudonym of "Publius," are only the most famous example of the outpouring of anonymous political writing that occurred during the ratification of the Constitution. Of course, the simple fact that the Framers engaged in certain conduct does not necessarily prove that they forbade its prohibition by the government. In this case, however, the historical evidence indicates that Founding-era Americans opposed attempts to

[366] *Id.* (citation omitted).

[367] *Id.* at 375 (Scalia, J., dissenting).

[368] I have previously drawn connections between this history and the prosecution of Wikileaks founder Julian Assange. *See* Jonathan Turley, Opinion, *How Likely Is an Assange Conviction in US?*, BBC NEWS (Apr. 11, 2019), https://www.bbc.com/news/world-us-canada-47874728 [https://perma.cc/Q5L3-S7HW].

[369] Jennifer B. Wieland, Note, *Death of Publius: Toward a World Without Anonymous Speech*, 17 J.L. & POL. 589, 591-92 (2001).

> require that anonymous authors reveal their identities on the ground that forced disclosure violated the "freedom of the press."[370]

Justice Thomas's concurrence highlights the dilemma that courts face in addressing challenges to the use of biometric technology. While supporting authors' right to anonymity, Justice Thomas qualifies his position by noting that the Framers' reliance on anonymity in such writings "does not necessarily prove that they forbade its prohibition by the government."[371] Biometric privacy will require a paradigm shift on anonymity from a component of either free speech or privacy toward a free-standing constitutional right connected to democratic values and activities.

The courts have grappled with the fact that databanks, cellular signals, and locational technology can now strip individuals of any sense of privacy regarding their movements. Dissenting in a pre-*Jones* case involving the warrantless installation of a GPS tracking device on a suspect's vehicle,[372] then–Chief Judge Alex Kozinski noted,

> You can preserve your anonymity from prying eyes, even in public, by traveling at night, through heavy traffic, in crowds, by using a circuitous route, disguising your appearance, passing in and out of buildings and being careful not to be followed. But there's no hiding from the all-seeing network of GPS satellites that hover overhead, which never sleep, never blink, never get confused and never lose attention. Nor is there respite from the dense network of cell towers that honeycomb the inhabited United States. Acting together these two technologies alone can provide law enforcement with a swift, efficient, silent, invisible and *cheap* way of tracking the movements of virtually anyone and everyone they choose.[373]

Until recently, the Supreme Court's jurisprudence in this area relied on distorted, outdated aspects of doctrines like the "third-party doctrine" that originated in *United States v. Miller*.[374] There the Court held that a person has no expectation of privacy in information given to a third party (in that case, a bank).[375] The flaws of this exception were made more evident in *Smith v. Maryland*.[376] There, the Court simply declared that the dialing of a phone number meant that a person who "voluntarily conveyed numerical information to the telephone company" had "no legitimate expectation of privacy in information . . . voluntarily turn[ed] over to third parties."[377] These rulings could

---

[370] *McIntyre*, 514 U.S. at 360-61 (Thomas, J., concurring in the judgment) (citation omitted).

[371] *Id.* at 360.

[372] United States v. Pineda-Moreno, 617 F.3d 1120, 1121 (9th Cir. 2010).

[373] *Id.* at 1126 (Kozinski, C.J., dissenting from denial of rehearing en banc).

[374] 425 U.S. 435, 440-42 (1976).

[375] *Id.*

[376] 442 U.S. 735 (1979).

[377] *Id.* at 743-44.

not have put privacy interests more at risk in the face of online transactions and communications spurred by new technology. Justice Sotomayor's concurrence in *Jones* is again insightful on this point.

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[378]

Seemingly in recognition of its poorly conceived third-party doctrine, the Court handed down a revision in *Carpenter v. United States*[379] by holding that police must secure a warrant to get locational information from cell phone providers—extending the scope of the expectation of privacy.[380] While the Court narrowly addressed only surveillance exceeding the seven days of data the government had accessed in the case,[381] it apparently recognized that, once again, technology had made a mockery of its prior doctrine. While not abandoning the third-party doctrine, the Court said, "Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection."[382]

Carpenter's discussion of general privacy interests is the most relevant to the question of biometrics' proper position in society. The Court first defined what it considers a protected interest in public movements before it addressed how cellular data can undermine that interest.

> A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." For that reason, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—

[378] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (citations omitted).

[379] 138 S. Ct. 2206 (2018).

[380] *Id.* at 2223.

[381] *Id.* at 2217 n.3.

[382] *Id.* at 2220.

> secretly monitor and catalogue every single movement of an individual's car for a very long period."[383]

The Court declared that the ability to track individuals in public contravenes a protected expectation of privacy. The Court also noted other elements with obvious significance for biometric privacy. The Court rejected the argument that there is no specific locational disclosure but merely data from which location can be inferred: "[T]he Court has already rejected the proposition that 'inference insulates a search.'"[384] The Court went further and reaffirmed the need to continue to review its doctrines in light of new technology, quoting *Kyllo* for the proposition that it "must take account of more sophisticated systems that are already in use or in development."[385] The Court noted that its doctrines can only reflect "the state of technology" at that time, though many of us have long questioned its third-party doctrine in general.[386] Nevertheless, *Carpenter* affirms a right to anonymous (or at least untracked) movements in public to some degree. The Court's decision, however, falls short of an embrace of a true anonymity right, particularly in its reservation that "[w]e do not . . . call into question conventional surveillance techniques and tools, such as security cameras."[387]

The recognition in the majority opinion in *McIntrye* that "[a]nonymity is a shield from tyranny of the majority"[388] holds considerable import for FRT and other biometric technology. This technology threatens to move citizens' privacy expectations from a baseline of relative anonymity in public to the type of fishbowl society that threatens continual recognition and surveillance. Uncontrolled technological growth creates a shifting foundation for the values discussed above insofar as it changes the context of protected conduct by changing citizens' expectations rather than directly changing speech or privacy. Yet, FRT constitutes one of the most radical technological shifts in history in terms of its expansion of the government's surveillance capabilities and the reduction of the citizens' expectations of privacy. FRT's growth will clearly have an impact on the variety of political process rights that figures like Meiklejohn and Ely sought to protect. The purpose of regulations should be to preserve the level of expectation of anonymity that fosters essential speech and associational rights. That protection can be established by regulating not just the use of FRT but also the databanks used for individual recognitions.

---

[383] *Id.* at 2217 (alteration in original) (citations omitted) (first quoting Katz v. United States, 389 U.S. 347, 351-52 (1967); then quoting *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment); and then quoting *Jones*, 565 U.S. at 430).

[384] *Id.* at 2218 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

[385] *Id.* (quoting *Kyllo*, 533 U.S. at 36).

[386] *Id.* at 2219.

[387] *Id.* at 2220.

[388] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

IV. RECOGNIZING OBSCURITY AND PROTECTING BIOMETRIC PRIVACY IN A NONYMOUS WORLD

Rather than living in a largely anonymous society, we live in a nonymous society where people are known by face and name on the Internet and social media. The social baseline has shifted due not only to government use of biometric technology but also to the increasing use of such technology. This trend is primarily driven by consumers rather than by the government. From precheck systems at airports to Intelligent Vehicle Highway Systems ("IVHS"),[389] consumers are embracing programs that allow access to their movements, identity, and even purchases. At the same time, the government has failed to stem the scourge of identity theft. Even companies like Equifax, despite pledging to protect credit records, have fallen victim to hacking and identity theft.[390] In this vulnerable environment, consumers are welcoming products that can identify them—a product trend that plays to the very weakness of the *Katz* expectation of privacy test. To put it simply, it will be difficult to make the "cat walk backwards" from an increasingly nonymous to an anonymous society.

A. *Anonymity Through Obscurity: Restoring Expectations of Public Privacy*

As the Court observed in *Griswold*, the "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance."[391] The Court could find the protection of anonymity (or a form of obscurity) within the penumbra of free speech and association. Of course, some on the Court would balk at protecting the penumbra of privacy which itself was penumbral. However, a fishbowl society is the antithesis of a host of rights under the Constitution and would create a society in which rights are guaranteed but their exercise largely deterred through surveillance. The foregoing analysis has explored three interests that could be the foundation for biometric privacy protections: traditional privacy, anonymity, and obscurity. Privacy, as we have discussed, is poorly suited to deal with the most contentious biometric elements, which occur primarily in public areas. As Professor Alan Westin noted, privacy is generally defined as "the voluntary and temporary withdrawal of a person from the general society through physical or

[389] Thomas B. Kearns, Note, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 995 (1999) ("IVHS is an interactive system in which travelers and their vehicles communicate with the roadway in an effort to 'reduce traffic congestion, improve highway safety, and reduce environmental harm from vehicular traffic.'" (quoting Sheri A. Alpert, *Privacy and Intelligent Highways: Finding the Right of Way*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 97, 97 (1995))).

[390] *See* Press Release, FTC, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [https://perma.cc/X7Q6-ZKCV].

[391] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

psychological means."[392] The interests raised by biometric privacy are fundamentally different. Where privacy is often embodied in an act of withdrawal or detachment, FRT and other biometric technology undermine the ability of individuals to engage and join. Thus, once a person is in public, the more relevant value is anonymity. However, anonymity will be increasingly difficult to protect from the inroads of technology. The question is, in our increasingly transparent society, whether there is a way to protect against the Hawthorne-like effects on democratic activities. The answer may be to focus not on anonymity but on obscurity as the goal for addressing biometric technology.

In her work on privacy, Professor Judee Burgoon identified four different types or dimensions of privacy: informational, social, psychological, and physical.[393] Classic privacy cases often focus on physical privacy and the steps taken to protect private conduct. Informational privacy is an emerging focus of legislation. Social privacy embodies those steps that we take to preserve intimate or confidential relationship and communications. Yet, it is psychological privacy that may be the most relevant interest for the purposes of FRT and other biometric technology. It is a more subtle sense of privacy that allows an essential type of freedom of thought. While not addressed by Burgoon, these technologies strike at the formulation of not just associations but also thought in public space. While freedom of thought is certainly exercised in private contemplative moments, some of our most formulative thoughts are constructed by moving within society with a sense of obscurity that gives us an ability to explore, engage, and experiment. It is that same freedom of obscurity that can impact the other dimensions because we acquire information and develop social connections in these public wanderings.[394] If society is to protect this broader dimension of privacy, it must be able to offer its own transparent guarantees that citizens will not be subject to identification and tracking in their everyday movements absent a court order or other formal protections. Only by formulating bright-line protections will individuals have the sense of freedom of thought and association in public that is so essential to a democratic society.

FRT and biometric technology force a reexamination through a fundamental shift in the use of public information. It is the combination of one's biometric

---

[392] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

[393] Judee K. Burgoon, *Privacy and Communication*, 6 ANNALS INT'L COMM. ASS'N 206, 210-32 (1982).

[394] In work related to privacy guarantees linked to personal autonomy, this broader and transformative role of privacy has been a focus of writers.

> Much more is involved here than the right to be let alone. What is at stake is the protection of concrete, fragile identities, and self-creative processes which constitute who we are *and* who we wish to be. When properly understood, privacy rights protect these as well as the chance for each individual to develop, revise, and pursue her own conception of the good—her identity needs.

Jean L. Cohen, *Redescribing Privacy: Identity, Difference, and the Abortion Controversy*, 3 COLUM. J. GENDER & L. 43, 101 (1992).

information with databanks that now allows for virtually instant disclosure of the citizens' identity and personal information. Jim Harper noted,

> Practical obscurity has long ensured that even nonprivate information is not widely shared. An endless array of social, legal, and economic practices has developed around the assumption that the information collected about people will remain practically obscure. The things we wear, the places we go, the people we see, the things we say, and the things we buy have all been chosen in the past under the umbrella of practical obscurity.[395]

FRT and biometric technology nullify this level of practical obscurity with searchable databases.[396] New private technology is rapidly eliminating anonymity even further. Clearview AI, a "tiny company," has reportedly devised a "groundbreaking facial recognition app."[397] To the alarm of privacy advocates, the app's code contains the ability to pair with augmented-reality glasses, which could allow users the potential "to identify every person they saw."[398] The app is designed to access a "database of more than three billion images that Clearview AI claims to have scraped from Facebook, YouTube, Venmo and millions of other websites," going beyond any other database built by the "United States government or Silicon Valley giants."[399] The company has offered free thirty-day trials to law enforcement agencies with great success; the Indiana State Police "solved a case within 20 minutes of using the app," and a New Jersey detective extolled the app for its ability to "identify a suspect in a matter of seconds."[400]

This rapid decline of anonymity in society magnifies the importance of obscuring measures. Citizens will increasingly expect to be identified in public, but the democratic interests in anonymity can still be achieved through obscurity. As a matter of law, citizens can be assured that the government will not biometrically confirm their public movements, either directly or indirectly (through private surveillance systems), absent probable cause of a felony offense.[401] That guarantee allows individuals to associate, organize, and advocate in public despite the saturated FRT environment.

---

[395] JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD 162 (2006).

[396] *See generally* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343 (2015) (utilizing concept of "obscurity," which deals with transaction costs involved in finding or understanding information, to understand why government surveillance is troubling).

[397] Hill, *supra* note 79.

[398] *Id.*

[399] *Id.*

[400] *Id.* (quoting Email from Robert Bracken, Deputy Lieutenant, Clifton Police Dep't, to Mark Centurione, Chief, Clifton Police Dep't (July 4, 2019, 7:24 AM) (on file with the Boston University Law Review)).

[401] *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (declining to "grant the state unrestricted access to a wireless carrier's database of physical location information").

While anonymity focuses on the identification of an individual, obscurity concerns the concealment of an otherwise recognizable identity. Accordingly, "[a]n individual is obscure to an observer if the observer does not possess or comprehend critical information needed to make sense *of* the individual."[402] The Supreme Court has already recognized how "practical obscurity" protects privacy.[403] In *Whalen v. Roe*, the Court considered privacy concerns over New York medical records and recognized the "threat to privacy" in such systems.[404] The Court made direct reference to the "practical obscurity" at work in *U.S. DOJ v. Reporters Committee for Freedom of the Press*,[405] in which it held that rap sheet information was protected from disclosure under the Freedom of Information Act ("FOIA"), even though it was made available from various government sources.[406] Ironically, it was the government that raised "practical obscurity" in opposing disclosures under the FOIA.[407] The Court held that

> [i]n addition to the common-law and dictionary understandings, the basic difference between scattered bits of criminal history and a federal compilation, federal statutory provisions, and state policies, our cases have also recognized the privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public.[408]

In holding that the rap sheet information could be withheld by the government, the Court quoted with approval the view of then-Justice Rehnquist that just because "an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[409]

Justice Rehnquist's effort to define a privacy interest in not wholly private information was incomplete precisely because it remained tethered to conventional privacy cases and theories built upon physical privacy notions. As Gavison observed, "[P]rivacy must have coherence as a value, for claims of legal protection of privacy are compelling only if losses of privacy are sometimes undesirable and if those losses are undesirable for similar reasons."[410] We simply lack that coherence for privacy interests in anonymous public movement and

---

[402] Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 5 (2013).

[403] *See id.* at 21.

[404] Whalen v. Roe, 429 U.S. 589, 605 (1977).

[405] 489 U.S. 749 (1989).

[406] *Id.* at 780.

[407] *Id.* at 762.

[408] *Id.* at 767.

[409] *Id.* at 770 (quoting William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?, or: Privacy, You've Come a Long Way, Baby*, 23 KAN. L. REV. 1, 8 (1974)) (noting that a substantial privacy interest exists in rap sheets, as modern computers can accumulate and maintain information that might otherwise have been forgotten).

[410] Gavison, *supra* note 288, at 423.

association. If we are to have a coherent system of biometric privacy protections, there must be either a new understanding of privacy as encompassing obscurity or the recognition of anonymity as a distinct and protected interest.

Addressing obscurity in the Internet context, Hartzog and Stutzman proposed that online communications are obscure—and therefore protected—if they are missing at least one of four factors that are essential for disclosure: search visibility, unprotected access, identification, and clarity.[411] Such protections are obviously far narrower than what is being discussed in this Article. Indeed, it is the "modest" aspect of their proposal that Hartzog and Stutzman view as one of its most promising characteristics.[412]

Their theory, however, pulls support from two broader works that are equally relevant to this Article's analysis. First, there is Nissenbaum's theory of privacy as contextual integrity.[413] Nissenbaum argues for protections based on the context in which information is disclosed or held. Nissenbaum postulates that people reveal information in "finely calibrated systems of social norms, or rules" from health care disclosures to political chat rooms.[414] This creates context-relative information norms that can be distinguished and protected in different ways. Nissenbaum's interesting work is well suited for the debate over Internet privacy. However, this Article explores the need for relative anonymity or obscurity in an individual's public movements as a whole. Where Nissenbaum's work resonates the most is in the context of recognition by private businesses. She posits that "there are no arenas of life *not* governed by *norms of information flow* . . . . Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation."[415] People will increasingly venture into stores and settings that use biometric recognition. However, they will do so with the understanding that such recognition is being used (and presumably waived their privacy interest) for a specific and limited marketing or customer care purpose. This is a new context in Nissenbaum's relative world of disclosures. As discussed below, we can protect this new context by codifying the use of the information to keep it in line with what Nissenbaum refers to as the "*norms of information flow*."[416]

Second, Professor Lior Strahilevitz's work also has particular relevance to this analysis. Strahilevitz's "A Social Networks Theory of Privacy" draws on

---

[411] *See* Hartzog & Stutzman, *supra* note 402, at 32.

[412] *Id.* at 41 (asserting that, although obscurity offers only modest privacy protections, it minimizes likelihood of discovery by specific individuals).

[413] NISSENBAUM, *supra* note 275, at 3 (introducing idea that the growth of technology has "provoked and continue[s] to provoke anxiety, protest, and resistance in the name of privacy").

[414] *Id.*

[415] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 137 (2004).

[416] *Id.*

common-law torts to theorize that protected expectations of privacy are often recognized through a lens of disclosure probability.[417] The thrust of his theory is that "[i]f it is theoretically possible, but extraordinarily unlikely, that information shared with a few individuals will ultimately become widely known by the public, then privacy tort law usually discounts the theoretical possibility and holds that the data privacy subject maintains a reasonable expectation of privacy."[418] This social networks theory suggests that a court can make a context-specific calculation based on how and to whom information is disclosed. Citizens can rest easy in the understanding that information can be narrowly shared with the reasonable expectation that it will not be shared beyond the circle of initial communicants.[419] Thus, Strahilevitz maintains that "[c]ourts simply need to ask themselves: was the widespread dissemination of this information inevitable, or did the defendant's actions materially affect the extent of subsequent disclosure?"[420]

The social network context of Strahilevitz's work limits its application to this Article's analysis of a general right to obscurity in public. However, there is an underlying notion that one can be lost in a crowd in public movements that is based on the expectation—and reality—that no single person that one encounters could piece together their every movement, expression, or speech. Observation is insular and discrete. It is possible to create systems that prevent the consolidation of such data points of public movement into a mosaic, as discussed below.

B. *Common-Law Privacy and Constitutional Norms as Limitations on Transparency-Forcing Technology*

The concept of anonymity through obscurity rests on the notion that people can have much of their lives accessible in bits of data found in a myriad of different databases. However, people can remain largely anonymous because of limits on combining those bits of information into a single profile.[421] On the

[417] *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 939-46 (2005) [hereinafter Strahilevitz, *A Social Networks Theory of Privacy*] (describing how, when the probability of information becoming public decreases, the probability that tort law finds a reasonable expectation of privacy increases); *see also* Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2039 (2010) [hereinafter Strahilevitz, *Reunifying Privacy Law*].

[418] Strahilevitz, *Reunifying Privacy Law*, *supra* note 417, at 2039; *accord* Hartzog & Stutzman, *supra* note 402, at 33-34.

[419] *See* Strahilevitz, *A Social Networks Theory of Privacy*, *supra* note 417, at 939-46 (discussing how "American law eschews a categorical answer to the question of under what circumstances a limited disclosure of private information about one's self renders that information 'public' for the purposes of tort law").

[420] *Id.* at 975.

[421] *See* Kearns, *supra* note 389, at 993.

Internet, it is obscurity rather than anonymity that protects most people.[422] Such obscurity has largely been lost through informational systems that use "computer matching," smart cards, and other consolidations of data.[423] We are rapidly approaching a post-privacy world in which privacy is gradually worn down by products that are irresistible for millions of consumers. It is possible to limit governmental use of FRT and other biometric technology to protect Fourth Amendment interests. However, the exponential expansion of transparency-forcing commercial products can make such Fourth Amendment protections mere pretenses of privacy. The irony is inescapable. For centuries, privacy has been in a constant struggle with security. As a relative abstraction, privacy routinely has lost ground to more concrete demands for government protection against terrorism or other threats. Since 9/11, we have become accustomed to rollbacks in privacy as new surveillance and data searches are implemented. Yet, courts have slowed that erosion and, at times, even regained some privacy ground.[424] The problem for biometric privacy is that the primary threat comes from commercial products and the appeal of transparency to consumers. Products like Google's face-matching programs offer concrete and immediate benefits against the abstract concerns of being transparent in one's association. As opposed to claims of the government that appeal to personal safety, these commercial products appeal to personal vanity and social interactions. The result is the same: privacy is dying through consensual waivers by popular demand.

As discussed earlier in Section III.C, the Supreme Court has often raised the potential chilling effect that government action has on the exercise of constitutional rights. However, the concern over the inhibition of protected conduct is often not determinative. The chilling effect in some cases will come not from the anticipation of government action but from private actions. Those cases can produce difficult balancing tests because limiting the chilling effect can result in curtailing countervailing private expression or association. The greatest threat presented by transparency-forcing technology lies in its use by private citizens and companies, particularly in products that allow for the recognition of an individual across the Internet. Restricting government use of biometric technology will achieve little in protecting public anonymity if citizens can be searched easily with private products that disclose public movement or associations. That will, however, push the chilling effect rationale beyond the farthest extent recognized by the Supreme Court.[425]

---

[422] *See* Hartzog & Stutzman, *supra* note 402, at 48.

[423] *Kearns*, *supra* note 421, at 993-94.

[424] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

[425] Notably, even when a case presents a chilling effect on constitutional conduct, the Court has tended to avoid relying heavily on that effect in rendering its decisions. Thus, in *Davis v. FEC*, 554 U.S. 724 (2008), the Court invalidated a law that stipulated that if a candidate spent more than the threshold of personal funds on a campaign, the candidate's opponent could spend three times the finance limit. *Id.* at 729. The Court noted that the law "requires a candidate to choose between the First Amendment right to engage in unfettered political

In *Doe v. Reed*,[426] the Supreme Court balked at the use of a chilling effect rationale to oppose a public records law that required the public release of signatures on ballot initiative petitions.[427] The plaintiffs brought a facial challenge to the law and argued that the publication of the names would trigger public harassment and abuse.[428] The ballot initiative petitions in question sought to reverse a law that benefited same-sex couples. However, "several groups plan[ned] to post the petitions in searchable form on the Internet, and then encourage other citizens to seek out the . . . signers."[429] The eight-Justice majority rejected the "scant evidence or argument beyond the burdens they assert disclosure would impose on . . . petition signers."[430] The mere threat of harassment was insufficient in balancing the state's interest in transparency against the risk of discouraging the participation in the political system.[431]

The skepticism the Court gave to the harassment exception in *Reed* does little to encourage those who want the Court to expand its cabined view of privacy in public movements and associations. Indeed, Justice Sotomayor joined the Justices in questioning the basis for limiting public access to such information, despite her later concurrence in *Jones* warning that the "[a]wareness that the government may be watching chills associational and expressive freedoms."[432] Balanced against the value of transparency in politics, the Justices found the fear of harassment or intimidation to be uncompelling. There are certainly distinctions to be drawn, particularly with the countervailing democratic participatory values raised in *Reed*. Yet, in an earlier ruling, *Buckley v. Valeo*,[433] the Court had recognized a potential chilling effect on political associations in challenges to campaign finance rules but did not find such an effect in the facts presented.[434] Indeed, the Court stated in *Buckley* that "[i]t is undoubtedly true that public disclosure of contributions to candidates and political parties will

speech and subjection to discriminatory fundraising limitations." *Id.* at 739. However, it emphasized that "[t]he resulting drag on First Amendment rights is not constitutional simply because it attaches as a consequence of a statutorily imposed choice" but rather because it "does not provide any way in which a candidate can exercise that right without abridgment." *Id.* at 739-40.

[426] 561 U.S. 186 (2010).

[427] *Id.* at 199-202 (holding that disclosure of petition signatories does not violate First Amendment).

[428] *Id.* at 199-200; *see also* Monica Youn, *The Chilling Effect and the Problem of Private Action*, 66 VAND. L. REV. 1471, 1534-37 (2013) (discussing *Reed* and the Court's history in using chilling effect rationale).

[429] *Reed*, 561 U.S. at 199.

[430] *Id.* at 201. While an as-applied challenge was still possible, the Court fractured on the reasoning and standard. *Id.* at 203 (Alito, J., concurring); *id.* at 218 (Stevens, J., concurring).

[431] *Id.*

[432] *Compare* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring), *with Reed*, 561 U.S. at 201.

[433] 424 U.S. 1 (1976) (per curiam).

[434] *Id.* at 74.

deter some individuals who otherwise might contribute."[435] While the Court left open the possibility of an as-applied challenge, it required a showing of "a reasonable probability that the compelled disclosure [of personal information] will subject [the individual] to threats, harassment, or reprisals from either Government officials or private parties."[436] The Court reaffirmed that standard in *Reed*.[437]

The *Buckley* standard of "reasonable probability" notably includes conduct from "private parties" and not just the government.[438] The Court also addressed the chilling effect of private conduct in *Brown v. Socialist Workers '74 Campaign Committee (Ohio)*,[439] in which it viewed the Socialist Workers Party's challenge to a state disclosure statute favorably to avoid the danger of the Party becoming "the object of harassment by government officials and private parties."[440] However, in *Reed*, the Court demurred in protecting individuals from the social or political consequences of participating in political acts. So, it is clear that the effort to protect public movements and associations could well fall on the wrong side of the same balancing test. As Monica Youn noted, these cases could be reconciled by the fact that some level of government action was involved, while establishing that "[t]he dividing line between the two categories [of governmental and private chill cases] turns on whether the government has violated a constitutional rule, not on the mere presence or absence of some level of private action."[441] The thrust of this view is that private chill cases are actionable if there is a threshold finding of a governmental violation of a constitutional rule that is magnified by private retaliation or harassment.[442] Thus, censorship-by-proxy cases like *NAACP v. Alabama ex rel. Patterson* can be explained not as protecting against private conduct but as being triggered by a government violation of a constitutional rule like the "state's violation of neutrality norms through invidious discrimination."[443]

The chilling effect of FRT and other biometric technology is more defused in its curtailment of privacy interests. The problem with transparency-forcing technology is that it creates the general fishbowl phenomenon, leading to a chilling effect in a host of potential political and social associations. One product already allows FRT to link with other pictures of an individual taken in public,

[435] *Id.* at 68.

[436] *Id.* at 74.

[437] *See Reed*, 561 U.S. at 196.

[438] *Buckley*, 424 U.S. at 74.

[439] 459 U.S. 87 (1982).

[440] *Id.* at 88.

[441] Youn, *supra* note 428, at 1502.

[442] *Id.* at 1503 (referring to requirement that there first be a finding of a violation of a constitutional rule as part of "a two-phase analysis").

[443] Youn, *supra* note 428, at 1504-05; *see also* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 463 (1958) ("The crucial factor is the interplay of governmental and private action . . . .").

creating a composite of movement.[444] This violates no clearly defined constitutional rule; indeed, the greatest risk of chill comes from private use of private commercial products. To protect obscurity as a constitutional value, the Court would need to depart significantly from these past cases in what can be framed as a conflict between private citizens over publicly observable conduct. The focus on the violation of a "constitutional rule" is a tad artificial absent agreement on what those rules are or where they are derived from. Constitutional values, including privacy, are defined not in the Constitution but in court cases and the common law.

The common law has long been used in defining constitutional values. Indeed, it is precisely the basis for Brandeis and Warren's "The Right to Privacy."[445] The article laid out how common-law traditions can be used to support both constitutional and statutory privacy protections. The nexus between common-law and constitutional rule has been recognized by both academics and jurists in a variety of areas. Indeed, David Strauss posited that "[i]n practice constitutional law is, mostly, common law."[446] Strauss noted that debates over the Equal Protection Clause invoke the principles of *Brown v. Board of Education*[447] and subsequent cases rather than the words of the Equal Protection Clause.[448] He also explained that the original understanding of the Sixth Amendment—that the government only may not forbid a defendant from having the assistance of counsel—has been superseded by the Supreme Court's decision in *Gideon v. Wainwright*[449] and subsequent decisions.[450] Strauss argued that this "common law constitutionalism" is actually superior to textualism and originalism in many respects.[451] The Supreme Court has often invoked the common law in reaching

[444] Hill, *supra* note 79.

[445] Warren & Brandeis, *supra* note 72, at 214.

[446] David A. Strauss, *Common Law Constitutional Interpretation*, 63 U. CHI. L. REV. 877, 904 (1996).

[447] 347 U.S. 483 (1954).

[448] Strauss, *supra* note 446, at 883.

[449] 372 U.S. 335, 344 (1963).

[450] Strauss, *supra* note 446, at 920; *see also* Bute v. Illinois, 333 U.S. 640, 660-66 (1948) (discussing common-law history of right to counsel).

[451] Strauss presents three major benefits of "common law constitutionalism" over competing theories. First, he asserts that judicial restraint is better served by such an approach because the common law has a "centuries-long record of restraining judges" given that the approach allows judges to openly and candidly address relevant moral and political views. Strauss, *supra* note 446, at 927. Second, the approach is at least broadly consistent with the demands of democracy given the development of important common-law principles that are widely held by society. Finally, the common law is aware of the undemocratic nature of judicial review and has built-in principles to protect from its abuse. *See* Strauss, *supra* note 446, at 926-34.

decisions on constitutional issues.[452] For example, the Supreme Court decision in *Gertz v. Robert Welch, Inc.*[453] was widely understood to "constitutionalize" the fair comment privilege, originally found in the common law, through dicta.[454] Similarly, states use common law to inform their own constitutional values. The Supreme Court of Utah explicitly recognized the "well established principle" that common-law sources must be examined to "discern the outer limits of the freedom of speech."[455] The New York Court of Appeals found that an analysis of New York's constitutional text and history is "informed by the common law."[456]

The common law has robust protections for privacy in torts like intrusion upon seclusion and publicity given to private life.[457] Additionally, individuals may sue for publicity given to private facts that "would be highly offensive to a reasonable person" and that are "not of legitimate concern to the public."[458] Those torts reflect a foundational value that is relevant in understanding the scope of constitutional rules. The intrusion upon seclusion tort largely protects nonpublic spaces and information. It provides no exception for "newsworthy" information. The New York Court of Appeals extended this protection to public spaces in *Nader* when the intrusion involved looking over the shoulder of the consumer advocate while he was filling out a bank deposit slip.[459] The second tort, giving publicity to private life, does contain a newsworthy exception and has more direct application to biometric privacy, including a possible exception for the use of FRT by media. Two questions remain, however: What is a "private fact"? And does it encompass public movement and associations?

As noted above, the traditional constructs of privacy do not easily lend themselves to biometric privacy protections. However, the expansion of private rights of action for cases involving FRT and other biometric technology is possible as notions of private facts evolve with new technology. Indeed, the Supreme Court has tailored such common-law actions in light of constitutional values. For example, in *New York Times Co. v. Sullivan*, the Court curtailed the

[452] *See, e.g.*, Missouri v. Holland, 252 U.S. 416, 433 (1920) ("The case before us must be considered in the light of our whole experience and not merely in that of what was said a hundred years ago.").

[453] 418 U.S. 323 (1974).

[454] *Id.* at 339-40; *see also* Ollman v. Evans, 750 F.2d 970, 975 (D.C. Cir. 1984) (en banc) (noting the Supreme Court's adoption of common law standard as a constitutional principle).

[455] *See* Am. Bush v. City of S. Salt Lake, 140 P.3d 1235, 1250 (Utah 2006).

[456] *See* Immuno AG v. Moor-Jankowski, 567 N.E.2d 1270, 1278 (N.Y. 1991) ("While we look to the unique New York State constitutional text and history, our analysis also is informed by the common law of this State.").

[457] *See supra* note 273 and accompanying text.

[458] RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977).

[459] Nader v. Gen. Motors Corp., 255 N.E.2d 765, 771 (N.Y. 1970) ("A person does not automatically make public everything he does merely by being in a public place, and the mere fact that [the plaintiff] was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing.").

scope of common-law defamation to protect a "breathing space" for free speech and the free press.[460] It recognized that such liability could create a chilling effect on constitutionally protected activities. The same was true in *Snyder v. Phelps*,[461] in which the Court curtailed the tort of intentional infliction of emotional distress to protect the right of the Westboro Baptist Church to protest the funeral of a soldier killed in the Iraq War.[462] Both of these cases resulted in the contraction of common-law torts to preserve space for free speech activities. However, it is also possible to expand such torts to encompass emerging and expanded definitions of privacy interests to protect such values, including privacy interests linked to the democratic process. Torts like giving publicity to private life could be interpreted to include the disclosure of movement and associations in public. That in turn would allow private enforcement of biometric privacy in actions against individuals and companies using FRT or other biometric technology to expose such information through Internet searches or other sources. Such civil actions could include injunctive relief as well as damages to protect biometric privacy.[463]

Any recognition of a common-law or constitutional right to obscurity is itself bounded by two countervailing interests. First, there is obviously a law enforcement interest that curtails privacy and free speech interests. With the protection of court orders, such balancing can still reinforce an expectation of privacy. Second, other constitutional values must be balanced against the interest of being obscure or publicly anonymous. This type of conflict was at the heart of the Court's decision in *Time, Inc. v. Hill*.[464] In that case, several Justices were clearly sympathetic toward the arguments of a family that a novel and a movie based on their being held hostage constituted a serious invasion of their privacy interests.[465] Juxtaposed to the privacy values was the countervailing interest of the First Amendment. As reflected in his decision in *Sullivan*, Justice Brennan embraced a robust view of free speech that mirrored the views of writers like Meiklejohn who connected that right to "[p]ublic discussions of

[460] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 271-72 (1964) (quoting NAACP v. Button, 371 U.S. 415, 433 (1963)).

[461] 562 U.S. 443 (2011).

[462] *Id.* at 457-58 (holding that speech on matter of public concern and on public street cannot be basis of liability for tort of intentional infliction of emotional distress, even if speech is interpreted as offensive or outrageous).

[463] For example, in 2020, Facebook reached a $550 million settlement for the use of FRT without consent in violation of the Illinois biometric law. Jeff Horwitz, *Facebook Reaches $550 Million Settlement in Facial-Recognition Lawsuit*, WALL STREET J. (Jan. 29, 2020, 8:26 PM), https://www.wsj.com/articles/facebook-reaches-550-million-settlement-in-facial-recognition-lawsuit-11580347594.

[464] 385 U.S. 374, 387 (1967).

[465] *See generally* Samantha Barbas, *When Privacy Almost Won:* Time, Inc. v. Hill, 18 U. PA. J. CONST. L. 505 (2015).

public issues."[466] In his opinion for the Court in *Hill*, Justice Brennan quoted from *Thornhill v. Alabama*[467] to explain that protecting free speech was not simply a matter of protecting political speech but all speech: "Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period."[468] The cushion of obscurity is the very "breathing space" that Brennan described as constitutionally guaranteed in his decision to limit the common-law torts.[469] Brennan emphasized that common-law torts had to be limited because of the chilling effect on free speech from the threat of liability. The fear was that such a threat would cause journalists to "steer . . . wider of the unlawful zone."[470] The associations and interactions enabled by free movement in public help form the ideas expressed in these cases. If citizens can be recognized or tracked in public, they will "steer wider" of any interactions that could cause embarrassment or difficulties in their private or professional lives.

In balancing the interests in these cases, Justice Brennan came down on the side of free speech and the free press over privacy values. The decision reaffirmed the "newsworthy" exception to privacy in the interests of protecting the critical role of free speech in a democratic society.[471] The balancing of interests in the biometric context would prove more challenging and interesting. The premise of this Article is that biometric privacy is key to preserving the same First Amendment interests embraced in *Hill* and *Sullivan*. By protecting biometric privacy, we can increase the breathing space for free speech and free association. Yet tensions will continue when limiting technology impacts other protected rights. Consider emerging products that allow searches of the Internet to match with a face print. A reporter could use FRT to track the movement of anyone deemed newsworthy like a celebrity, a political dissident, or a politician. There is ample reason for the United States and the European Union to ban the sale or use of such products.[472] The technology would radically increase the ability to scan photos visually—an enhancement that is analogous to the earlier GPS or thermal imagery cases.[473] While the Supreme Court is inclined toward balancing tests, the lower courts have interpreted newsworthiness quite broadly. It takes little to justify such interest. Moreover, it is impractical for the Court to protect situational public anonymity for citizens in such conflicts. The value of

[466] Alexander Meiklejohn, *The First Amendment Is an Absolute*, 1961 SUP. CT. REV. 245, 257.

[467] 310 U.S. 88 (1940).

[468] *Hill*, 385 U.S at 388 (quoting *Thornhill*, 310 U.S. at 102).

[469] New York Times Co. v. Sullivan, 376 U.S. 254, 271-72 (1964).

[470] *Hill*, 385 U.S. at 389 (alteration in original) (quoting *Sullivan*, 376 U.S. at 279).

[471] *Id.* at 400.

[472] *See* Turley, From Here to Obscurity, *supra* note 105, at 11-18.

[473] *See, e.g.*, United States v. Jones, 565 U.S. 400 (2012); Kyllo v. United States, 533 U.S. 27 (2001).

free movement is to forego views and associations to avoid the chilling effect of the threat of recognition. The only effective way to give "breathing space" in public movement is to bar the use of technology that would create a mosaic of all appearances of an individual from images mined from social media or the Internet.[474]

While such common-law values could be significant in protecting biometric privacy, it is also obvious that changes in constitutional doctrine will have their greatest impact on government actions, which are the focus of First and Fourth Amendment analysis. For a broader level of regulation of this technology, these common-law and constitutional values will have to be expressed in the legislative form of a biometric privacy act.

C. *Codifying a Bounded Rationality of Public Privacy*

The rapidly expanding range of biometric products limits the effectiveness of constitutional challenges under the First and Fourth Amendments. Moreover, the high degree of consent to biometric monitoring and authentication programs further undermines such constitutional means for protecting biometric privacy and the democratic process values discussed above. Instead, we need to look for legislative and regulatory means to carve out a nonymous public space in anonymous society if we are to protect these democratic values. It is possible to craft protections for biometric privacy without denying the increasingly nonymous society that citizens are embracing. The alternative is stark and inevitable. Ubiquitous monitoring and recognition will become a fact of life and citizens will be identified as they shop, work, or travel. The bases under *Katz* for any expectation of anonymity and traditional privacy will fall accordingly with the spread of this technology. However, it is possible to statutorily create a type of obscurity that focuses on the danger to the democratic process. By limiting the access to and utilization of FRT and other biometric technology by the government, it is possible to obscure the movement of individuals who are readily identified. Based on the popularity of FRT products, the preference of most individuals is most likely to be a type of situational obscurity where they can rely on privacy in certain circumstances in which they are most concerned about how images might affect their reputations or status. Certainly, it is possible to protect certain situations with added protections like courts or controlled settings. That will not, however, achieve the goals of protecting the democratic values discussed earlier. To protect those values will require a more universal obscurity guarantee in public movements absent individual concern.

The erosion of biometric privacy through consensual acts highlights the need to create statutory protections like a proposed national Biometric Privacy Act. It will also require the evolution of constitutional, statutory, and common-law protections to protect the right to obscurity under the First Amendment. That will not protect against consensual waivers (which a legislative act can regulate), but it can lay a constitutional foundation for the architecture of a right to

[474] *See Sullivan*, 376 U.S. at 272.

obscurity or public anonymity. Such a right has an important defining role for citizens in understanding their akratic choices as consumers. The Constitution does not protect citizens from bad choices, but it can better define the scope and consequences of those choices.

The absence of a clearly defined protection for a public privacy right impacts not only the scope of government privacy conduct but also private choices.[475] Psychologist Herbert Simon explained how such structure frames choices of individuals in a "bounded rationality," writing,

> If we wish to know what form gelatin will take when it solidifies, we do not study the gelatin; we study the shape of the mold in which we are going to pour it. In the same way, the economist who wishes to predict behavior studies the environment in which the behavior takes place, for the rational economic actor will behave in whatever way is appropriate to maximize utility in that environment. Hence (assuming the utility function to be given in advance), this maximizing behavior is purely a function of the environment, and quite independent of the actor.
>
> The same strategy can be used to construct a psychology of thinking. If we wish to know how an intelligent person will behave in the face of a particular problem, we can investigate the requirements of the problem. Intelligence consists precisely in responding to these requirements.[476]

Simon's "bounded rationality" explored how human conduct and choices change in a given environment.[477] Constitutional structure can have the same role in creating a bounded rationality in defining and protecting core rights like privacy or anonymity in public spaces.[478] An example of how laws frame attitudes and expectations is found in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its privacy rule.[479] Due to HIPAA postings and regulations, citizens have been assured (and expect) protected health information measures from doctors and hospitals. If we are to avoid a post-privacy world, it will require the isolation of the underlying right to such anonymity not just for the Court but also for the public. With the added legislative and regulatory structure, consumers can better understand the implications of biometrics waivers. Bounded rationality also shows how

---

[475] *See generally* Jonathan Turley, *A Fox in the Hedges: Vermeule's Vision of Optimized Constitutionalism in a Suboptimal World*, 82 U. CHI. L. REV. 517 (2015) (book review); Jonathan Turley, *Madisonian Tectonics: How Form Follows Function in Constitutional and Architectural Interpretation*, 83 GEO. WASH. L. REV. 305 (2015).

[476] Herbert A. Simon, *Invariants of Human Behavior*, 41 ANN. REV. PSYCHOL. 1, 6 (1990).

[477] HERBERT A. SIMON, MODELS OF THOUGHT 1 (1979); *see also* Christine Jolls & Cass R. Sunstein, *Debiasing Through Law*, 35 J. LEGAL STUD. 199, 200 (2006) ("To the extent that legal rules are designed on the basis of their anticipated effects on behavior, bounded rationality is obviously relevant to the formulation of legal policy.").

[478] *See generally* Dan M. Kahan, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, 67 U. CHI. L. REV. 607 (2000).

[479] 42 U.S.C. § 1320d-2 (2018).

structure and anchoring can influence human perception and conduct. Constitutional values can provide such structure and anchoring. At the moment, no such anchoring exists in a largely wide-open context for FRT and other biometric products and programs.[480]

The creation of a Biometric Privacy Act is the more direct and promising means for protecting the values discussed in this Article. Common-law and constitutional values can heavily influence such a law as they did when the Supreme Court's rulings on electronic surveillance became a blueprint for a comprehensive legislative regimen. In *Berger v. New York*,[481] the Court reviewed the New York surveillance law and found various constitutional deficiencies that were then used as the foundation for Title III of the Omnibus Crime Control and Safe Streets Act of 1986.[482] The specific provisions of the Act are the focus of another work.[483] However, a few broad components of a possible Title 55 for biometric privacy are worth emphasizing.

Controversies continue to mount in the patchwork system of federal and state laws governing the use of biometric technology. Maryland state officials recently admitted that ICE officials have run facial-recognition searches on millions of Maryland driver's license photos without first receiving state or court approval.[484] The chief information officer for Maryland's Department of Public Safety and Correctional Services provided no details about who was given access to the database, the reasons for the searches, or who was identified.[485] Similarly, recently released documents indicated that the FBI may have scanned millions of Americans' license photos without their knowledge or consent and without authorization from Congress or state legislatures.[486]

---

[480] Such legislation is no easy legal or political task. In January 2020, the European Commission revealed that it was considering issuing a moratorium on the use of FRT in public areas for up to five years in a draft of its White Paper on Artificial Intelligence. *Facial Recognition: EU Considers Ban of Up to Five Years*, BBC NEWS (Jan. 17, 2020), https://www.bbc.com/news/technology-51148501 [https://perma.cc/3NBS-LFFD]. A month later, facial recognition was almost entirely omitted from the final draft, coinciding with reports that people feared the ban would "stifle innovation and compromise national security." Amrita Khalid, *The EU's Agenda to Regulate AI Does Little to Rein in Facial Recognition*, QUARTZ (Feb. 20, 2020), https://qz.com/1805847/facial-recognition-ban-left-out-of-the-eus-agenda-to-regulate-ai/ [https://perma.cc/LK8J-RY2A]; *see also Commission White Paper on Artificial Intelligence - a European Approach to Excellence and Trust*, at 21-22, COM (2020) 65 final (Feb. 19, 2020).

[481] Berger v. New York, 388 U.S. 41 (1967).

[482] *Id.* at 62-64; *see also* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197.

[483] *See* Turley, From Here to Obscurity, *supra* note 105, at 16.

[484] Drew Harwell & Erin Cox, *ICE Given Free Rein on Md. Driver's License Data*, WASH. POST, Feb. 27, 2020, at A1.

[485] *Id.*

[486] Drew Harwell, *FBI, ICE Tap into License Photos*, WASH. POST, July 8, 2019, at A1.

As a threshold matter, any effort to create a protected space for biometric privacy would require the preemption of state laws. The Illinois BIPA[487] is a leading example of state experimentation in regulating this expanding market. Texas[488] and California[489] also have enacted laws regarding their state limits and liabilities. Those states alone represent a significant percentage of both commerce and population in the United States. A variety of other states are moving toward the enactment of their own laws. Cases brought under these laws have national reach in their potential monetary and injunctive relief. As with command and control statutes like the Clean Air Act and market-based statutes like the Sherman Act, biometric privacy is an interstate problem demanding a single, comprehensive national approach. Biometric technology is used on the Internet and has a classic interstate profile for regulation by Congress. The worst possible approach to regulation is the creation of a patchwork of different state laws with different approaches to privacy protections. Not only would that system present an unfair environment for businesses using these products but also it would not create the stable bounded rationality that is needed to reinforce privacy expectations. To achieve the objective of reinforcing key expectations of privacy in public movements and associations, a Biometric Privacy Act would also have to include limits on both public and private uses of FRT and other biometric technology. While the Supreme Court should extend Fourth Amendment protections, including the warrant requirement, to biometric searches, Congress can also require such protections as it did with Title III. In this way, law enforcement would be allowed to have FRT and other biometric capabilities but would be required to show probable cause to use this technology to find a wanted felon. Thus, if the police have probable cause supporting the identification of a murder suspect, they could secure a warrant to allow access to live FRT systems in locating the individual in public. A law would also stipulate conditions and protections governing government biometric databanks, limiting access and barring the transfer of data absent the satisfaction of defined conditions.

A national legislative solution would also need to create a regulatory platform compatible with recent European regulations of biometric technology. There is currently a vacuum created by the lack of any comprehensive U.S. law on biometrics. The enactment of such an act would allow the United States to work on a global approach to these products and their applications. In 2016, the EU enacted Regulation 2016.679 on "the protection of natural persons with regard to the processing of personal data and on the free movement of such data."[490] The EU regulations define biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the

[487] 740 ILL. COMP. STAT. 14/1 to /99 (2020).

[488] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019).

[489] CAL. CIV. CODE § 1798.100-.199 (West 2020).

[490] Council Regulation 2016/679, 2016 O.J. (L 119) 1 (emphasis omitted).

unique identification of that natural person, such as facial images or dactyloscopic data."[491] While there is a clear need to develop laws and regulations compatible with the EU's, there are some potential areas of conflict. The EU regulation remains broadly written but allows nations to adopt their own specific rules. It includes a massive potential exception that could swallow the rule for disclosures of "[p]ersonal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest."[492] One area of commonality could be the creation of a required system for express and specific consent for the use of face prints and images. The EU requires such consent in products, though its enforcement is far from clear. A U.S. biometric law could require a uniform consent "box" for industry that requires individuals to agree to the sharing of their images within a company or the sharing of such images.

Consent provisions highlight the greatest challenge to national legislation. Absent significant regulations of private biometric technology, the regulation of government programs would be virtually meaningless in creating a protected space for public movement and associations. For example, citizens will hardly feel protected from monitoring if, while the government requires court orders to track their movements, any private individual could use commercial programs to search social media and the Internet for any 1:N program match of a person's face. Such programs could show that individuals attended rallies or associated in public with different groups. This little brother surveillance could easily eclipse government surveillance and establish the fishbowl society that civil libertarians want to avoid. Yet, limitations on government biometric systems are relatively easy to impose in comparison to the regulation of private biometric systems.

To some extent, the statutory limits on private biometric technology would have to rely on the very biometric technology they seek to control. First and foremost, a consent scheme would require a hash or a type of digital watermark that would attach to a photo to prevent its transfer or use beyond the scope of consent. Such technology exists, but it will require a national—and preferably international—system of recognition. Likewise, legislation could bar the use of consent conditions for Internet-wide FRT searches as a condition for employment. Finally, many uses of FRT and biometrics by businesses cannot practically use express consent rules—for example, a retail store using the technology to identify customers or shoplifters. It is possible to accept that, with signage notice of the use of FRT or other biometric technology, entering a store can be accepted as consent. However, this should be conditioned on other national protections including a bar on sharing such data and spoilage dates when existing face prints are deleted after a specific, and preferably short, period of time.

[491] *Id.* at art. 4, § 14.

[492] *Id.* at art. 86.

An EU-compatible act would also allow FRT and other biometric technology to be used more effectively for identity authentication. While often portrayed as a technology inimical to individual rights and privacy values, FRT and other biometric technology could play a critical role in greatly reducing identity theft. This could be achieved by requiring a two-factor authentication for certain online or banking transactions. Likewise, an act could mandate national standards, developed by NIST, for products to address concerns over erroneous identifications based on race and gender.[493] The standard test should be required for all FRT with an emphasis on the racial discrimination concerns. Every product sold in the United States should be certified under the NIST test with published accuracy scores for consumers. Such publications alone would place considerable legal and market pressures on these companies. Alternatively, businesses using a low-scoring product would be more vulnerable to lawsuits for discrimination or other injuries associated with false matches, particularly when better performing products are available. Other biometric products, like voice identification, could also be subject to such mandatory testing with public posting of performance results.

These types of provisions can create the bounded rationality needed to establish a valid expectation of privacy—or at least obscurity—in public movements and associations. With increased recognition of the need for such obscurity as a constitutional value part of a democratic society, a Biometric Privacy Act could codify these values in a transparent system of consent and regulation of the use of biometric technologies for both public and private uses.

CONCLUSION

Robert Merton once wrote that "'[p]rivacy' is not merely a personal predilection; it is an important functional requirement for the effective operation of social structure."[494] Merton's work reflected both a normative and instrumental basis for privacy protections. This Article attempted to isolate instrumental values of anonymity or obscurity from our democratic system and examine how those values can be meaningfully protected. FRT and other biometric technology present obvious threats to privacy and the political process. These technologies promise transformative change in both legal and social realities for citizens. For generations, one of the greatest protections of civil liberties has been the technological and practical barriers. A government simply could not surveil and monitor large numbers of citizens. That technological horizon is vanishing with the advent of computers, data banks, and affordable high-resolution cameras. The protection of public anonymity could be achieved with a shift in Supreme Court precedent—much like the corrective moves in cases like *New York Times v. Sullivan* and *Carpenter v. United States*. Even if the Supreme Court is unwilling to abandon its treatment of public spaces

[493] *See* Bushwick, *supra* note 172.

[494] ROBERT K. MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 429 (enlarged ed. 1968).

as largely unprotected from public surveillance, Congress could protect anonymity interests.

The functionalist defense of biometric privacy will not satisfy many who value privacy as a normative value in and of itself. The Court has repeatedly defended privacy in the home on a loosely normative basis but dismissed such claims once an individual ventures into public. A normative argument for anonymity in public is too easily dismissed as an absurd argument that people—and particularly police—should avert their eyes from making any recognition. Using the traditional privacy approach, the loss of privacy is likely to accelerate with new transparency-forcing technology. We could easily find ourselves in a de facto post-privacy world. If that occurs, Phyllis McGinley will be correct that having a "withdrawing place" may become a luxury of the rich in a transparent world.[495]

While the statutory elements will be likely fiercely debated, a Biometric Privacy Act can be crafted to protect individuals in their public movements and associations as well as their Internet associations.[496] However, if we are to reach a consensus on such elements, we need to clearly define what we are protecting and why. The democratic values of anonymity cannot be seriously denied. The question is how to protect those democratic values when society is turning away from anonymity. The answer proposed by this Article is to build FRT- and other biometric-privacy-based protections around the model of obscurity. It is possible in a nonymous society to codify a level of obscurity as opposed to anonymity. After all, the most important interest in anonymity is the protection of the democratic process and engagement.[497] By codifying a type of "anonymity by obscurity," we can create the guarantee sought by many citizens that the government will not be allowed to gather recognition data on public events without a tailored and specific warrant seeking an individual.

Such protections are premised on the basic need for human development and democratic processes to be obscure. FRT threatens to reproduce the Hawthorne Effect exponentially—changing not just how citizens act but also how they *interact*. Even the possibility of constant recognition and tracking can have a pronounced impact on personal development. To be unable to move around society without being effectively followed denies a certain space for growth and exploration. Put another way, people have always lost themselves in a crowd. That invisibility allows them to observe, and even role-play, in a way that would be chilled by observation. This is evident on the Internet where people use anonymity to voice views that they would never utter in known company. Sometimes such anonymity produces negative consequences like the expression

---

[495] *See* MCGINLEY, *supra* note 261, at 56.

[496] *See* Turley, From Here to Obscurity, *supra* note 105.

[497] In the balancing of interests with privacy, the importance of privacy to the democratic process has rarely been weighted by courts or commentators, with a few exceptions. *See, e.g.*, SOLOVE, *supra* note 294, at 50; James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 7 (2003).

of once-suppressed racist or hateful views. Yet, it can also be used by people exploring their sexuality and by individuals adopting new political or social associations while protected in the armor of anonymity. With the onslaught of transparency-forcing technology, it is not clear if we can go back to true anonymity by obscurity in society. We can make recognition less chilling by limiting the use and sharing of biometric data by private and government parties. In this way, biometric technology becomes more like the observation of strangers on the street—an observation with limited memory and use. That may be the best that can be done when citizens themselves are surrendering anonymity.

For better or worse, citizens are changing their views on recognition technology. They see a value in giving up anonymity and traditional privacy values to achieve other benefits. Ironically, one of the most common benefits is to protect one's identity by making it more easily authenticated. Presented with increasing threats of identity theft (and a dismal record of the government combatting such crime), citizens view FRT and other biometric technology as a way of protecting their own identities. As a result, recognition technology is becoming a part of modern life as privacy continues to evolve with social norms. The question is whether academics can confidently state that a more absolute view of privacy is the normatively correct position even if the social norms contradict that view.

Biometric technology will force society to deal with what we are working to protect in public forums. This is a distinctly descriptive or instrumental approach to privacy. However, this approach provides a better understanding of the specific threat of this technology that can be lost in the thrill of recognition programs from cellphones to airport security gates. The success of biometric products will soon become a menace to society if we cannot reach a consensus on what we can protect and how we can protect it. A Biometric Privacy Act could achieve a level of obscurity even in a nonymous society. The rough outline of this Article is merely an effort to frame such a debate on what we are protecting and how we might structure such protections.

Any progress on biometric privacy will require a comprehensive reexamination of what interests we are seeking to protect in our new nonymous world, including the limits of traditional privacy definitions. The notion of a "withdrawing place" reflects the inherent human need to be alone. However, there is also a human need to be part of a society and to be among people. It is not simply the notion of being "lost in a crowd" but also the ability to explore and experiment in human interactions. It is not a withdrawing but an engaging place, and it defines not just individuals but ultimately the society within which they exist. If that zone of safe interaction and exploration is lost, the impact on society—particularly a democratic society—could be as tragic as it is transformative.