THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOLUME XXV STLR.ORG FALL 2023

ARTICLE

PUBLIC PERCEPTIONS CAN GUIDE REGULATION OF PUBLIC FACIAL RECOGNITION

Matthew B. Kugler*

Facial recognition technology is changing how people pass through customs at airports, check in at schools, and move anonymously in public spaces. Yet despite these transformations, its use by the government is largely unregulated. This Article informs the policy and doctrinal debates about facial recognition by presenting a public attitudes perspective. These three novel empirical studies show the nuanced views that Americans hold about government use of facial recognition. The data reveal that people are generally comfortable with the government using facial recognition to investigate serious crimes, enhance the security of controlled spaces like airports and schools, and increase the efficiency of identity verification in some contexts. But people are often not comfortable with casual governmental facial recognition use in public spaces. This pattern of strong comfort for tailored uses persisted even when, in a second study, participants were primed with negative information about the accuracy of facial recognition. Here I explore the implications of these results for both current Fourth Amendment doctrine as well as future legislative reform, promoting a balanced approach that allows tailored use of facial recognition while regulating its purposes.

* Professor of Law at Northwestern Pritzker School of Law. Thanks to Andrew Ferguson, Aziz Huq, Sara Katsanis, Hajin Kim, David Schwartz, Nadav Shoked, and Roseanna Sommers for their comments on earlier versions of this Article, to the faculty of the University of Denver for their feedback. Special thanks to background research by Allison Lee and general cleanup by Matt Choi.

I. INTRODUCTION

"The use of facial recognition technology poses a staggering threat to Americans' privacy." - Senator Ed Markey, 2019[1]

The US government has been using facial recognition for a wide variety of purposes and its use is likely to expand in the future.[2] At the same time, scholars and civil rights organizations have raised concerns regarding the technology's accuracy, its impact on marginalized communities, and its consequences for the reach of government authority.[3] News reports of mistaken arrests,[4] use in airports,[5]

---

[1] Janosch Delcker & Cristiano Lima, *Fight Against Facial Recognition Hits Wall Across the West*, POLITICO (Dec. 13, 2019, 5:03 PM), https://perma.cc/325F-N84T; @SenMarkey, TWITTER (Jul. 14, 2019, 2:22 PM), https://perma.cc/46WW-HT8G.

[2] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-526, FACIAL RECOGNITION TECHNOLOGY CURRENT AND PLANNED USES BY FEDERAL AGENCIES (2021) [hereinafter AUGUST 2021 GAO REPORT].

[3] *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105 (2021); *See also* Lindsey Barrett, *Ban Facial Recognition Technologies for Children - And for Everyone Else*, 26 B.U.J. SCI. & TECH. L. 223, 241 (2020); Drew Harwell, *Civil Rights Groups Call on Biden to Halt Federal Use of Facial Recognition Technology*, WASH. POST (Feb. 18, 2021), https://perma.cc/8CBU-P4R8.

[4] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[5] Geoffrey A. Fowler, *TSA Now Wants to Scan Your Face at Security. Here Are Your Rights*, WASH. POST (Dec. 2, 2022, 7:00 AM), https://perma.cc/N2LQ-JYMJ.

and facial identification via social media[6] have opened the public's eyes to the nearly unlimited future possibilities of this technology.

Facial recognition puts law in an uncomfortable position. If one focuses on the mechanism of facial recognition—the mere comparison of one image to another—then it is hard to see what the problem is. Humans have checked identification cards and compared photographs for as long as identification cards and photographs have existed. Facial recognition merely makes the process faster. But the problem is clear if one focuses on the consequences of an effective and broadly-deployed facial recognition system. Suddenly a person cannot walk down a public street without having the event recorded and preserved for posterity. Anonymity in public becomes a thing of the past.

The government has recognized this difficulty. In May 2022, President Biden issued an executive order requiring the study of government use of facial recognition technology.[7] Other actors, at varying levels of government, have sought to introduce new regulations of facial recognition.[8] But, as of now, there is little consensus on what such regulation should look like.

This Article presents three novel empirical surveys that investigate the public's attitudes about the government's use of facial recognition technology for both law enforcement and non-law enforcement purposes. The surveys reveal that the public holds highly nuanced views of this important technology, and they suggest a path forward for future regulation. Ultimately, the Article promotes a tiered approach for facial recognition. Non-law enforcement uses would generally be permitted so long as they were narrow and targeted or in controlled-access spaces. Law enforcement uses would be permitted only with a warrant and only for more serious offenses, borrowing from provisions in the Wiretap Act.

Right now, there is little government regulation of facial recognition.[9] The federal government has yet to pass any laws restricting its use, and state and local governments have only scattered provisions.[10] Constitutionally, it is challenging to regulate facial recognition under the Fourth Amendment. Faces are generally

---

[6] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[7] Exec. Order No. 14,074, 87 Fed. Reg. 32,945 (May 25, 2022).

[8] *See, e.g.*, Facial Recognition Act of 2022, H.R. 9061, 117th Cong. (2022); Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. (2019).

[9] *See infra* Part I.C.; *See also* Barry Friedman, *Law Enforcement's Facial Recognition Law-lessness: Comparing European and U.S. Approaches*, JUST SECURITY (Mar. 10, 2020), https://perma.cc/2J82-GER2.

[10] *See* Jameson Spivack & Clare Garvie, *A Taxonomy of Legislative Approaches to Face Recognition in the United States*, A.I. NOW INST. 86, 90–92 (Sept. 2020), https://perma.cc/JDP8-82GC.

viewed as public.[11] Even were the Supreme Court to treat facial recognition as a special case—as it did cell phone location data[12]—it would be confronted with the difficult line-drawing question. Is every use of facial recognition a Fourth Amendment search, or only some uses? Is live monitoring of a city's cameras different from the identification of an isolated photo of a criminal suspect?

There is also a broad range of governmental uses of facial recognition that have nothing to do with criminal law enforcement. How are those to be handled? Facial recognition has been used for airport security and customs control, for identity verification in public schools, and as an anti-fraud mechanism in administering public benefits.[13] Should these uses be permissible? Even were facial recognition held to be a Fourth Amendment search, warrantless use of it in these cases might still be constitutionally acceptable under the special needs doctrine.[14]

I believe that consideration of public attitudes and expectations can inform this regulatory process and that public expectations are directly relevant to some of the doctrinal questions that will face courts. First, public attitudes can inform policy via the legislative process. A legislative body seeking to pass new privacy laws may wish to learn the extent to which the opinions of the public mirror the well-honed perspectives of advocacy groups.[15] Are people as concerned as breathless news headlines would suggest?[16] Or are people generally trusting of government and law enforcement action in this context? Or are they concerned about some uses but generally trusting of others?[17] This last possibility, which is what the data here show, means that neither privacy advocates nor privacy skeptics has the puzzle entirely solved.

Second, public attitudes can inform the legal and policy questions via doctrine. Though current black letter law has little to say about the use of facial recognition in public places, the law can change. Many scholars have advocated using public opinion data to inform the Fourth Amendment's reasonable expectations of privacy analysis, meaning that public attitudes in favor of facial recognition regulation should affect the doctrinal analysis. Writing with Lior Strahilevitz, I argued that use

---

[11] U.S. v. Dionisio, 410 U.S. 1, 14 (1973).

[12] Carpenter v. U.S. 138 S. Ct. 2206, 2217 (2018).

[13] *See infra* Part I.A.

[14] *See infra* Part I.C.

[15] *See, e.g.*, Ashley Del Villar & Myaisha Hayes, *How Face Recognition Fuels Racist Systems of Policing and Immigration–and Why Congress Must Act Now*, ACLU (July 22, 2021), https://perma.cc/Q4WB-2AST; Adam Schwartz, *Resisting the Menace of Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 26, 2021), https://perma.cc/55S3-S7Z9.

[16] For a discussion of the abolitionist or trap perspective on police surveillance, *see generally* Andrew Guthrie Ferguson, *Surveillance and the Tyrant Test*, 110 GEO. L.J. 205, 230-34, 240 (2021) ("An uncompromising abolitionist would end the debate here: banning police technology and policing as we know it.").

[17] For a discussion of the "default" of trust in law enforcement, *see generally* Ferguson, *supra* note 17, at 214-20.

of such data is entirely consistent with the current doctrinal framework.[18] Professors Christopher Slobogin and Joseph Schumacher pioneered an empirical method of measuring public attitudes by having respondents rate the intrusiveness of a variety of law enforcement information-gathering techniques.[19] More recently, a large number of scholars have investigated Americans' opinions and beliefs about forms of electronic surveillance. They have found, for example, that people generally expect privacy in data, such as their cell phone location records.[20] Under these theories, public attitudes are directly relevant to Fourth Amendment doctrine in the criminal investigation context.

Public attitudes may also affect the constitutionality of non-law enforcement use of facial recognition. Outside of the law enforcement context, the constitutionality of a surveillance regime is assessed under the "special needs" doctrine.[21] The core of that doctrine is a freeform reasonableness analysis that, broadly speaking, weighs the intrusiveness of the search against the government's reasons for conducting it.[22] Public attitudes are one indication of the reasonableness of a search.[23] They point to whether or not people generally feel that a search intrudes upon their privacy.

Part I reviews the current state of facial recognition technology in the U.S. It considers how facial recognition is actively being employed by the government now as well as uses that are on the horizon. It then assesses the concerns raised about facial recognition and the generally lax state of facial recognition regulation. It closes by examining the problem of line-drawing in the case of this powerful and emerging technology.

Part II presents the results of three novel empirical studies. The results show that respondents' comfort with government use of facial recognition is highly context-driven. People report being generally comfortable with the government

---

[18] For an extensive discussion justifying the use of such data, *see generally* Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 224-44 (2016).

[19] Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 736-37 (1993); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 110–11 (2007); *see also* Jeremy A. Blumenthal, Meera Adya & Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331, 343–45 (2009) (replicating Slobogin and Schumacher's main results).

[20] *See, e.g.*, Christine S. Scott-Hayward, Henry F. Fradella & Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 45–58 (2015); Bernard Chao, Catherine Durso, Ian Farrell & Christopher Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 301 (2018).

[21] *See* Ill v. Lidster, 540 U.S. 419 (2004); *see also* Matthew B. Kugler & Mariana Oliver, *Constitutional Pandemic Surveillance*, 111 J. CRIM. L. & CRIMINOLOGY 909, 912 (2021).

[22] *See, e.g.*, Skinner v. Railway Lab. Execs. Ass'n, 489 U.S. 602, 619 (1989); *see also* Kugler & Oliver, *supra* note 22, at 912.

[23] *See* Slobogin & Schumacher, *supra* note 20, at 732; *see also* Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1189–91 (2014).

using facial recognition to investigate serious crimes, enhance the security of controlled spaces like airports and schools, and increase the efficiency of identity verification in some contexts. They also draw little distinction between using facial recognition to identify a stored image of a criminal suspect and scanning live feeds to try to locate the suspect. There were few differences in the views of different demographic groups—race, ethnicity, and gender had little relationship to comfort with facial recognition. And this pattern of comfort with targeted uses persisted even when, in a second study, participants were primed with negative information about the accuracy of facial recognition.

Yet people do have some concerns about facial recognition. They are often not comfortable with casual governmental facial recognition use. For example, most people do not think that merely being on a public street or in a public park should subject a person to facial recognition monitoring. So comfort with specific uses of facial recognition should not be mistaken for comfort with general or universal uses. And people are particularly uncomfortable with potential abuses.

To fully respect this context sensitivity, a statutory solution is needed. Part III comments briefly on the Fourth Amendment implications of the results and then addresses in more detail the contours of a statutory proposal for regulation of government facial recognition use. For non-law enforcement uses, the results suggest that general or universal facial identification in public spaces by the government intrudes unduly on privacy. Merely being in a public space does not justify this form of technologically-aided identification. Using facial recognition to help secure or monitor a space already subject to access restrictions, however, is likely reasonable and should be legal. For law enforcement uses, people's comfort levels changed based on the nature of the crime. Respondents were comfortable with the use of facial recognition only for the investigation of serious crimes. In response to these findings, I propose a legislative solution, akin to the Wiretap Act, that would permit the use of facial recognition in investigations for only serious crimes with procedural protections varying in stringency according to the facial recognition technique used.

II. THE PAST, PRESENT, AND FUTURE OF GOVERNMENT USE OF FACIAL RECOGNITION

Government actors are increasingly using facial recognition technology for a variety of purposes.[24] This section reviews the current state of facial recognition, summarizes how the U.S. government is currently using facial recognition and may plan to use it in the future, and then considers some of the common critiques and concerns raised by these uses. This evaluation will set the stage for the empirical studies described in Part II, which evaluate public perceptions of government facial recognition use.

---

[24] *See* AUGUST 2021 GAO REPORT, *supra* note 3.

A. Background on Facial Recognition and Governmental Uses

Facial recognition is a form of artificial intelligence that compares facial images. It is commonly divided into "one-to-one matching" and "one-to-many matching." "One-to-one matching" is a comparison of one facial image to another facial image. "Is the person presented here Bob, for whom I have a stored image?" This is also sometimes called facial *verification*. Alternatively, "one-to-many matching" is a comparison of one facial image to an array of other facial images. "Is the person presented here in my array of faces? If so, which image do they match?" Facial images can be taken from still photographs, stored video footage, live video footage, or a live person. This is sometimes called facial *identification*.

One-to-one matching is simply the automation of a process that could be easily conducted by a human being. One-to-many matching is a force multiplier. It may attempt to match the target person or image with a small number of alternatives, perhaps the 40 people expected in a class or on a plane, or a very large number, perhaps the entire contents of a state driver's license database. A facial recognition algorithm could evaluate whether a given image matches any of an arbitrary large number of comparison photographs in a small fraction of the time it would take a human to conduct the same task.

The United States Government has deployed facial recognition in a variety of settings.[25] Generally speaking, the government has used facial recognition in three main ways: (1) law enforcement investigations, (2) security at government offices and facilities, and (3) identity verification for fraud detection or convenience purposes.[26] Many of the United States Government's uses of facial recognition are similar to those of private entities and individuals.[27] Moreover, looking at the examples of the private sector and other countries provides some guidance on the kinds of uses that the U.S. Government could conceivably adopt in the near-term future.[28]

---

[25] *Id.* at 6–7.

[26] *Id.*; *See generally* DAVID FREEMAN ENGSTROM, DANIEL E. HO, CATHERINE M. SHARKEY & MARIANO-FLORENTINO CUÉLLAR, GOVERNMENT BY ALGORITHM: ARTIFICIAL INTELLIGENCE IN FEDERAL ADMINISTRATIVE AGENCIES (2020), https://law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf.

[27] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-621, FACIAL RECOGNITION TECHNOLOGY – COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 7–10 (2015).

[28] *See, e.g.*, Sam Shead, *UK Court Finds Facial Recognition Technology Used by Police Was Unlawful*, CNBC (Aug. 11, 2020, 10:12 AM), https://perma.cc/L724-QJWT; Melissa Locker, *Brazil Is Using a Facial Recognition System During Rio's Carnival*, FAST COMPANY (Jan. 30, 2019), https://www.fastcompany.com/90299268/brazil-is-using-facial-recognition-tech-during-rios-carnival.

1. Law Enforcement Use

Both federal and state law enforcement have used facial recognition. The Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) both use their own internal facial recognition programs.[29] The scope of local facial recognition capacities is less clear. At least twenty-six states permit law enforcement to run facial recognition scans using their state ID databases.[30] As of 2016, at least one out of four state or local law enforcement agencies were able to run facial recognition searches on their own or through another agency's system,[31] but a more recent article on police surveillance technologies found that about 10% of police departments claim to have facial recognition access.[32]

One law enforcement use of facial recognition is identification of a person who is either in custody or otherwise in the presence of a police officer. If the police apprehend an individual suspected of a crime and are unable to identify them, they can take a photo of them and use facial recognition to compare that photograph to a database of stored photos (e.g., mugshots, driver's licenses, juvenile booking photos).[33] This type of facial recognition is akin to fingerprinting or swabbing for DNA.[34] The ability to identify the suspect via facial recognition technology, in turn, helps to generate leads for criminal investigations.[35]

More broadly, law enforcement has already begun using facial recognition to identify suspects and generate investigative leads. Police departments across the United States have used facial recognition to compare photographs or live individuals to a government database (such as a state driver's license database or a

---

[29] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-518, FACIAL RECOGNITION TECHNOLOGY: FEDERAL LAW ENFORCEMENT AGENCIES SHOULD BETTER ASSESS PRIVACY AND OTHER RISKS 14 (2021) at 42-43, 48-50 [hereinafter JUNE 2021 GAO REPORT].

[30] Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://perma.cc/ZS24-TCWR.

[31] *Id.*

[32] Mariana Oliver & Matthew B. Kugler, *Surveying Surveillance: A National Study of Police Department Surveillance Technologies*, 54 ARIZ. ST. L.J. 103, 129–32 (2022).

[33] *See, e.g.*, Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html; Ferguson, *supra* note 4, at 1112-13.

[34] Ferguson, *supra* note 4, at 1113.

[35] Garvie, Bedoya & Frankle, *supra* note 31; Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 4:19 AM), https://perma.cc/Y9WC-FRA9 ("The technology has since crept across the country, to Los Angeles, San Diego, Chicago and New York, as well as hundreds of state and local law enforcement agencies."). Privacy advocacy group, Fight for the Future, has created an interactive map that attempts to visualize how widespread and common the use of facial recognition technology by law enforcement is in the United States. The website allows users to filter and refine the map based on what kinds of facial recognition uses they would like to see mapped out. *Ban Facial Recognition*, FIGHT OF THE FUTURE, https://perma.cc/ZNA7-8K2Q/ (last visited Jan. 31, 2023).

mugshot database).[36] Looking outside the United States, police in the United Kingdom and Brazil have experimented with live facial surveillance, using cameras that are equipped with facial recognition for real-time identification on city streets.[37]

Police have not only used facial recognition in connection with state and other government databases, but they have also applied the technology to publicly-available social media sites. One particularly famous—and controversial—example is law enforcement's use of Clearview AI.[38] Clearview AI claimed to have a database of more than 3 billion pictures of people's faces scraped from a variety of public-only web sources such as Facebook, Instagram, and LinkedIn.[39] Law enforcement officials are able to upload a picture of an unidentified or unknown individual into Clearview AI, and the software then tries to make the image with one of the company's stored images.[40] Indiana detectives have used Clearview AI to identify minors who are featured in exploitative videos and photos.[41] Task forces in Florida and South Dakota, Immigration and Customs Enforcement's (ICE) Homeland Security Investigations division, and the Royal Canadian Mounted Police have used the service to produce leads regarding child exploitation crimes.[42] During the Freddie Gray protests in Baltimore, police ran protestors' social media posts through "facial recognition systems to locate protestors with outstanding warrants."[43]

Cities and counties around the United States have also applied facial recognition to stored footage from local business security cameras and city-owned cameras. The Detroit Police Department's (DPD) use of facial recognition on stored city

---

[36] JUNE 2021 GAO REPORT, *supra* note 30, at 14. *See also*, Clare Garvie & Laura M. Moy, *America Under Watch*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://perma.cc/RF5K-SJBJ; *Inside the NYPD's Surveillance Machine*, AMNESTY INT'L, https://perma.cc/2DF5-WHAH (last visited Jan. 31, 2023).

[37] Shead, *supra* note 29; Locker, *supra* note 29; *Police to Roll Out Live Facial Recognition Cameras in London*, CNBC (Jan. 24, 2020, 9:03 AM), https://perma.cc/7KRE-6AWA.

[38] *See* Ryan Mac et al., *Surveillance Nation*, BUZZFEED NEWS (Apr. 9, 2021, 7:52 PM), https://perma.cc/74WB-YTWH.

[39] *Id.*; *See also Accelerate Your Investigations*, CLEARVIEW AI, https://perma.cc/M94R-G8MN (last visited Jan. 31, 2023).

[40] Hill, *supra* note 7.

[41] Kashmir Hill & Gabriel J.X. Dance, *Clearview's Facial Recognition App Is Identifying Child Victims of Abuse*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html.

[42] *Id.*; Jared Council, *ICE Signs Contract with Facial Recognition Company Clearview AI*, WALL ST. J. (Aug. 14, 2020, 8:52 PM), https://perma.cc/FDN5-FGYY; Andrew Russell, *RCMP Used Clearview AI Facial Recognition Tool in 15 Child Exploitation Cases, Helped Rescue 2 Kids*, GLOB. NEWS (Mar. 10, 2020, 11:37PM), https://perma.cc/M8P7-2JVF.

[43] Russell Brandom, *Facebook, Twitter, and Instagram Surveillance Tool Was Used to Arrest Baltimore Protestors*, THE VERGE (Oct. 11, 2016,1:42 PM), https://perma.cc/W9PG-FFWS.

camera footage is a notable example of this law enforcement practice. Through Detroit's Project Green Light Detroit Initiative, DPD can connect cameras installed at businesses, health clinics, schools, and apartment buildings to its facial recognition software.[44] DPD is then able to identify individuals caught on tape by seeing whether they are a match to an individual in Detroit's mugshot database.[45] Outside of Detroit, civil rights groups have also criticized the New York Police Department for its extensive network of surveillance cameras and its ability to link the city's cameras to its facial recognition software.[46]

Other countries have made even more expansive use of facial recognition for law enforcement purposes. Some countries have used live facial scanning to identify wanted persons or persons of interest. Between 2017 and 2019, the South Wales Police used a facial recognition software called "AFR Locate," which automatically scanned pedestrians' faces and compared them to databases containing images of persons of interest.[47] Similarly, the London Metropolitan Police announced in 2020 that they would scan crowds in specific locations in London in real time, comparing individuals to the Metropolitan Police's watchlists.[48] In Brazil, the City of Rio de Janeiro used facial recognition through the city's pole cameras "to identify people who have arrest warrants issued in their names" during Rio's Carnival.[49] Though this kind of live-tracking technology has not yet been commonly deployed in the United States, these examples show that it is technologically feasible.[50]

2. Security

In addition to its uses for law enforcement purposes, the United States Government has also used facial recognition to monitor controlled environments and verify access permissions.[51] These kinds of uses more closely mirror some of what is done in the private sector: basic identity verification that would previously have been done by human agents. In this way, United States Customs and Border Patrol (CBP) and the Transportation Security Administration (TSA) have both used facial recognition to confirm the identity of travelers.[52] Certain school districts around the country have experimented with facial recognition for verifying

---

[44] Garvie & Moy, *supra* note 37.

[45] *Id.*

[46] *Inside the NYPD's Surveillance Machine*, *supra* note 37.

[47] Shead, *supra* note 29.

[48] *Police to Roll Out Live Facial Recognition Cameras in London*, *supra* note 38.

[49] Locker, *supra* note 29.

[50] *See, e.g.*, Jon Schuppe, *Facial Recognition Gives Police a Powerful New Tracking Tool. It's Also Raising Alarms*, NBC (July 30, 2018, 3:08 AM), https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936.

[51] AUGUST 2021 GAO REPORT at 7.

[52] JUNE 2021 GAO REPORT at 49, 52.

individuals entering their schools.[53] The federal government has rolled out facial recognition for employee verification and employee access.[54] Private companies and spaces have also used facial recognition for security purposes in ways that the government is likely to adopt, including identifying persons of interest at large events,[55] banned individuals at casinos,[56] or known shoplifters as part of retail store security.[57]

Facial recognition is widely used in U.S. airports. As of July 2022, CBP has deployed facial recognition at thirty-two U.S. airports for verifying the identities of U.S. and international travelers.[58] When a traveler enters an international airport for entry into or exit out of the United States, the traveler "pause[s] for a photo at the [airport's] primary inspection point."[59] The camera then matches a live photo of the traveler with the photographic gallery.[60] The photographic gallery is created from information taken from travel manifests and other traveler information and photographs pulled from CBP databases.[61] Once the camera determines that the traveler is a match, the traveler may proceed.[62] TSA is also experimenting with using facial recognition for domestic flights and has conducted demonstrations of

---

[53] Ava Kofman, *Face Recognition is Now Being Used in Schools, But It Won't Stop Mass Shooting*, INTERCEPT, (May 30, 2018, 11:36 AM), https://theintercept.com/2018/05/30/face-recognition-schools-school-shootings/.

[54] *See, e.g.*, JUNE 2021 GAO REPORT at 47.

[55] Gabrielle Canon, *How Taylor Swift Showed Us the Scary Future of Facial Recognition*, GUARDIAN (Feb. 15, 2019 6:00 AM), https://www.theguardian.com/technology/2019/feb/15/how-taylor-swift-showed-us-the-scary-future-of-facial-recognition (Taylor Swift's security team using facial recognition to identify stalkers during her concert tour).

[56] Thomas Brewster, *Israeli Facial Recognition Once Did Border Checks in The West Bank. Now It Snoops on Casinos Across America*, FORBES (Sept. 1, 2022, 10:22 AM), https://www.forbes.com/sites/thomasbrewster/2022/09/01/oosto-israel-facial-recognition-surveillance-on-casinos-in-america/?sh=3ccd70ce4131 (Oklahoma casino using facial recognition to check casino visitors' faces against a watchlist of barred individuals).

[57] Kim Hart, *Facial Recognition Surges in Retail Stores*, AXIOS (July 19, 2021), https://www.axios.com/2021/07/19/facial-recognition-retail-surge.

[58] U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-106154, FACIAL RECOGNITION TECHNOLOGY CBP TRAVELER IDENTITY VERIFICATION AND EFFORTS TO ADDRESS PRIVACY ISSUES 3 (2022), https://www.gao.gov/assets/gao-22-106154.pdf.

[59] *CBP Completes Simplified Arrival Expansion at All US Airports*, U.S. CUSTOMS AND BORDER PROT. (Jun. 2, 2022), https://www.cbp.gov/newsroom/national-media-release/cbp-completes-simplified-arrival-expansion-all-us-airports.

[60] *Id.*

[61] JUNE 2021 GAO REPORT at 49; U.S. CUSTOMS AND BORDER PROT., DHS/CBP/PIA-056 TRAVELER VERIFICATION SERVICE PRIVACY IMPACT ASSESSMENT 5 (2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

[62] *Id.*

a facial recognition machine called CAT-2 for traveler verification purposes.[63] As of 2022, TSA has rolled out CAT-2 machines at thirteen airports.[64]

Several school districts have implemented facial recognition to verify individuals associated with their schools for security purposes.[65] In 2018, the school district of Lockport, New York announced it would be equipping its school buildings with Aegis, a security program provided by a Canadian company called SN Technologies.[66] The software can verify that individuals entering the school are students or staff and monitor for the presence of people on a blacklist, for example gang members, sex offenders, suspended students, or terminated employees.[67] Following Governor Cuomo's December 2020 moratorium on facial recognition in New York public schools, the District has ceased using Aegis.[68]

In 2019, another facial recognition company called AnyVision ran a weeklong pilot program at the Santa Fe Independent School District in Texas.[69] Like Aegis software, AnyVision's "Better Tomorrow" uses a watchlist to detect people of known concern (e.g., sex offenders) entering schools.[70] Cameras capture images of all people entering schools, which the software then compares to its database of stored photos (of students, teachers, employees, etc.) and its watchlist.[71] Texas City High School also purchased AnyVision's software and has used it at its stadium for

---

[63] JUNE 2021 GAO REPORT at 52.

[64] Ashley Mackey, *TSA Introduces New Facial Recognition Technology at LAX*, ABC (Mar. 18, 2022), https://abc7.com/new-airport-technology-tsa-precheck-process-facial-recognition/11662799/.

[65] Kofman, *supra* note 54.

[66] Kofman, *supra* note 54; *Products*, SN TECH., http://www.sntechnologies.ca/product/ (last visited Jan. 31, 2023.)

[67] *See also* Shelby Brown, *Facial Recognition Tech Coming to New York School District Next Week, Report Says*, CNET (May 31, 2019, 7:17 PM), https://www.cnet.com/news/privacy/facial-recognition-tech-coming-to-new-york-school-district-next-week/; *Products*, *supra* note 67; Kofman, *supra* note 54; *Aegis 'School Shooter' Facial Detection System Sparks Row*, BIOMETRIC TECH. TODAY, July 2019, at 2, https://www.sciencedirect.com/science/article/pii/S0969476519300918; Tim Fenster, *Trying for More Secure Schools: Lockport District Turning to Facial Recognition Software*, LOCKPORT J. (Mar. 4, 2018), https://www.lockportjournal.com/news/local_news/trying-for-more-secure-schools-lockport-district-turning-to-facial/article_f1cc9cfa-0898-5da0-ac5d-d600df21bed7.html.

[68] Caroline Haskins, *The New York School District That Used Facial Recognition Now Has to Stop*, BUZZFEED NEWS (Dec. 23, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/new-york-stops-school-facial-recognition.

[69] Alfred Ng, *This Manual for a Popular Facial Recognition Tool Shows Just How Much the Software Tracks People*, MARKUP (July 6, 2021), https://themarkup.org/privacy/2021/07/06/this-manual-for-a-popular-facial-recognition-tool-shows-just-how-much-the-software-tracks-people.

[70] *Id.*

[71] *Id.*

school events.[72] On one occasion, the software was able to detect the presence of an expelled student who showed up to his sister's graduation.[73] As of 2019, WIRED had identified eight public-school systems using facial recognition systems (including Lockport and Texas City).[74]

The federal government has also used facial recognition to verify government employees and ensure that only certain personnel are permitted into higher-security areas. The Federal Bureau of Prisons (BOP) uses facial recognition called the "Facial Recognition Access Control System" to verify the identity of their employees with special security clearance.[75] The Facial Recognition Access Control System enables BOP to authenticate entry into secure network operations centers (i.e., computer rooms) at some of their facilities.[76] The software uses facial recognition to verify their employees' identities for permissive entry purposes.[77] The Government Services Administration (GSA) has also discussed the potential for outfitting certain GSA doors with facial recognition capabilities that would allow only certain personnel to enter.[78]

3. Fraud prevention and convenience

Both federal and state governments have used or contemplated using facial recognition to speed up the process of obtaining or accessing government benefits while simultaneously reducing fraud. The Internal Revenue Service (IRS) briefly deployed facial recognition to verify the identities of taxpayers as they filed their taxes, but due to public backlash, it decided to provide a live interview option in lieu of the facial recognition verification.[79] At least two dozen states, however, have contracted with the company ID.me for unemployment benefit identity verification purposes.[80] Unemployment benefit recipients upload pictures of their government

---

[72] Tim Simonite & Gregory Barber, *The Delicate Ethics of Using Facial Recognition in Schools*, WIRED (Oct. 17, 2019, 6:00 AM), https://www.wired.com/story/delicate-ethics-facial-recognition-schools/.

[73] *Id.*

[74] *Id.* Since then, at least Marion County in West Virginia has added facial recognition. *See also* Mike Nolting, *Local Tech Company Adds Additional Security Layer at Marion County Schools*, METRONEWS (Aug. 2, 2022, 8:54 PM), https://wvmetronews.com/2022/08/02/local-tech-company-adds-additional-security-layer-at-marion-county-schools/.

[75] JUNE 2021 GAO REPORT at 46.

[76] *Id.*

[77] *Id.* at 25.

[78] *See Touchless Tools – Technology Interactions Without Physical Contact*, TECH AT GSA, https://tech.gsa.gov/techradar/technologies/touchless-tools (last visited Jan. 31, 2023

[79] *Press Release: IRS Announces Transition Away from Use of Third-Party Verification Involving Facial Recognition*, IRS (Feb. 7. 2022), https://www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition.

[80] Kim Lyons, *Facial Recognition Software Used to Verify Unemployment Recipients Reportedly Doesn't Work Well*, VERGE (Jun. 19, 2021, 2:30 PM), https://www.theverge.com/2021/6/19/22541427/facial-recognition-software-verify-

documents and a selfie video to the ID.me app.[81] The app's facial recognition then verifies whether the images from the government documents and the selfie are a match.[82]

Hospitals have also used facial recognition to prevent patient identity fraud and to speed up the check-in process. The Virginia Health Center announced that it will be implementing a facial recognition-based identification system at its hospital for patient intake.[83] The facial recognition system will be integrated with the hospital's existing electronic health record and administrative systems.[84] It is conceivable that the use of facial recognition at hospitals for patient check-in could expand to the use of facial recognition on unconscious or non-responsive patients who come to the hospital and are unable to provide information on their identities.[85] Authorities in the United States and the United Kingdom, for example, have used facial recognition to identify unconscious and deceased individuals.[86]

To help protect public safety during the COVID-19 pandemic, government entities made some services and processes remote and used facial recognition to verify users. For example, the California State Bar Association contracted with ExamSoft—a company that provides facial recognition-based verification

---

unemployment-benefits-id-me. CNN published a map of the 25 states using ID.me. *See* Rachel Metz, *Want Your Unemployment Benefits? You May Have to Submit to Facial Recognition First*, CNN NEWS (Jul. 23, 2021, 2:40 PM). https://www.cnn.com/2021/07/23/tech/idme-unemployment-facial-recognition/index.html.

[81] Metz, *supra* note 81; Dave Gershgorn, *21 States Are Now Vetting Unemployment Claims with a 'Risky' Facial Recognition System*, ONEZERO (Feb. 4, 2021), https://onezero.medium.com/21-states-are-now-vetting-unemployment-claims-with-a-risky-facial-recognition-system-85c9ad882b60. ID.me has posted an instructional video on how to use the app to verify your identity for unemployment benefits. The instructions state, "You'll be asked to look at the colors on your phone screen while ID.me takes a short selfie video." ID.me, *Verifying Your Identity for Unemployment Benefits*, YOUTUBE (Jan. 15, 2021), https://www.youtube.com/watch?v=n8O8ItZWUMM. Another FAQ from ID.me instructs selfie uploaders to "Hold the phone in front of your face to scan it then wait until you see a green check mark." The instructions are next to a GIF of someone moving their phone around their face while the screen changes colors until a green check mark appears. *How Do I Take and Submit a Selfie?*, ID.ME, https://help.id.me/hc/en-us/articles/360061369314-How-do-I-take-and-submit-a-selfie- (last visited Jan. 31, 2023

[82] *See* Metz, *supra* note 81; Gershgorn, *supra* note 82.

[83] Sun Gazette Newspapers, *Hospital Group Moves into Facial-Recognition Efforts*, SUN GAZETTE (Jun. 13, 2022).

[84] *Id.*

[85] *See* Katsanis et al., *A Survey of U.S. Public Perspectives on Facial Recognition Technology and Facial Imaging Data Practices in Health and Research Contexts*, PLOS ONE 16(10): e0257923 6 (Oct. 14, 2021), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0257923.

[86] *See, e.g.*, Jenny Rees, *Facial Recognition Technology Meant Mum Saw Dying Son*, BBC (Feb. 20, 2021), perma.cc/TLH4-54ST; JUNE 2021 GAO REPORT at 14.

services—to confirm the identities of remote California Bar Exam takers.[87] Due to racial bias and disparate impact concerns, civil rights groups challenged the California State Bar's choice to rely on facial recognition to prevent cheating, but the California State Bar chose to proceed with the technology.[88] California, however, is not alone in using facial recognition to confirm bar exam takers' identities during the pandemic: Connecticut, Massachusetts, New York, Ohio, Tennessee, Vermont, and Michigan also used facial recognition for bar exam verification purposes.[89]

Lastly, other countries have used facial recognition for voter verification to facilitate remote voting during the COVID-19 pandemic. Canada's Liberal Party used facial recognition as part of its federal candidate selection process so its members could verify themselves and then vote online during the pandemic.[90] Afghanistan also used biometric machines equipped with facial recognition to verify voters in its 2019 presidential elections.[91]

B. Concerns about facial recognition

In light of the vast range of current and planned government uses for facial recognition, scholars, activists, and the public writ large have voiced concerns about the technology's potential harms.[92] A number of U.S. cities and counties have even passed ordinances banning or imposing moratoria on the technology while assessing its risks and relative value.[93] There are several species of concern. One is that government use of facial recognition will create and exacerbate surveillance, privacy, and free speech issues. Another is that facial recognition will have a disparate impact on people of color, women, non-binary individuals, and children, among others, in part due to lower accuracy when identifying members of those

---

[87] Sam Skolnik, *Civil Rights Group Threatens Suit over Bar Exam Facial Scan*s, BLOOMBERG LAW (Feb. 10, 2021, 4:44 PM), https://perma.cc/YRV3-T4QJ.

[88] *Id*.; Debra Cassens Weiss & Stephanie Francis Ward, *Afternoon Briefs: California Bar Responds to Disparate Impact Allegation Regarding Facial Recognition Technology*, ABA J., (Feb. 17, 2021, 4:45 PM), perma.cc/LB64-9YJ9.

[89] Allie Reed, *Online Bar Exams Come with Face Scans, Bias Concerns*, BLOOMBERG LAW (July 28, 2020, 4:01 AM), perma.cc/Y3VZ-BPMF.

[90] Dirk Meissner, *Facial Recognition Use by Federal Liberal Party Raises Issues Here, Says B.C.'S Privacy Commissioner*, CBC (June 25, 2021, 7:57 PM), perma.cc/NP8Q-SJZC.

[91] Rod Nickel, *Biometric Machines in Afghan Vote Improve After Last Year's Glitches*, REUTERS (Sept. 28, 2019, 8:04 AM), perma.cc/93PV-8ML3.

[92] *See* Ferguson, *supra* note 4; Janosch Delcker, *Fight Against Facial Recognition Hits Wall Across the West*, POLITICO (Dec. 13, 2019, 6:57 PM), perma.cc/7ECP-8WR2; Drew Harwell, *supra* note 4.

[93] Spivack & Garvie, *supra* note 11, at 90–92; Ferguson, *supra* note 17, 234–235 (collecting examples).

communities.[94] A third concern is the possibility that government actors with access to the technology may abuse it for personal and inappropriate purposes. These last two concerns are heightened by the relatively low level of oversight and regulation in this area. Finally, there may be unique data security risks associated with the collection of facial recognition data.

1. Universal or Ubiquitous Surveillance

From a privacy perspective, facial recognition expands the government's gaze over the public by enabling the government to identify individuals with much greater ease.[95] In this way, facial recognition erodes "practical obscurity," or "the notion that, when information is hard or unlikely to be found, it is relatively safe."[96] No police investigation will involve an officer or team of officers comparing a suspect's photo to the hundreds of thousands or millions of images in a state's driver's license database manually; the amount of effort involved would be far too high. But with facial recognition, such a comparison would be swift. Even compared to other biometric technologies, facial recognition poses unique surveillance harms to the populace due to the ubiquity of facial images (as opposed to palm prints or fingerprints) and the ease of observing faces in most public settings.[97]

Apart from its use in criminal investigations, government surveillance using facial recognition also threatens free speech, associational freedoms, and personal autonomy.[98] The government could use facial recognition to identify protestors, for example, which would chill free expression.[99] And actual application of facial recognition is not the only danger. Protester conduct could be changed by the mere knowledge that the government *could* use facial recognition.[100] For example, it was

---

[94] Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280, Nat'l Inst. of Standards and Technology (Dec. 2019), perma.cc/YQ8U-LKMW.

[95] *See* Barrett, *supra* note 4, at 240.

[96] *Id.*; Woodrow Hartzog, *Body Cameras and the Path to Redeem Privacy Law*, 96 N.C. L. REV. 1257, 1290-91 (2018).

[97] Barrett, *supra* note 4, at 241 ("Photographs are used far more widely for identification, allowing the creation of databases from photographs collected for different purposes.").

[98] Ferguson, *supra* note 4, at 1198 ("Free expression, association, petitioning for redress, and political dissent all will be negatively impacted by face surveillance systems."); Barrett, *supra* note 4, at 243–44.

[99] *See* Rosalind Adams, *Hong Kong Protesters Are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched*, BUZZFEED NEWS (Aug. 17, 2022, 6:01 AM), perma.cc/6KYB-DNMA; Ferguson, *supra* note 4, at 1198 ("Police have already shown a willingness to use surveillance technologies to monitor dissenting voices, and face surveillance will only strengthen that power."); Michael Kwet, *The Microsoft Police State: Mass Surveillance, Facial Recognition, And The Azure Cloud*, The Intercept, (July 14, 2020, 3:42 PM), perma.cc/9BYB-RFNJ; Barrett, *supra* note 4, at 243–244.

[100] Barrett, *supra* note 4, at 243–44.

widely publicized that protestors were identified by the Chinese government after a round of anti-regime protests in 2022.[101] This possibility weighed heavily on some of those identified as they considered future protests. One protestor said the ordeal left him "terrified" and that it would "be very difficult to mobilize people again."[102]

Furthermore, if facial recognition becomes too pervasive, scholars fear that the technology could interfere not only with people's political activities, but also with their associational freedom more broadly.[103] People may feel as if they are being tracked and restrain their lifestyle choices accordingly.[104] Identification through facial recognition could permit authorities to potentially see whatever information is linked to that individual, including criminal history, religion, or political affiliation.[105] Relatedly, government use of facial recognition on social media sites may result in "context collapse" "wherein people—unable to determine the appropriate social norm or cue due to countless audiences and unknowable expectations—simply default to certain self-presentation strategies to cope, including self-censorship, disengagement, and others forms of self-restraint."[106] By indirectly or directly restricting people's freedom of expression, government use of facial recognition could ultimately hinder personal autonomy and development.[107]

Moreover, scholars suggest increased deployment of facial recognition could shift people's sense or expectations of privacy in public, thereby changing social norms.[108] This gradual erosion of privacy expectations is particularly plausible given the possibility of mission creep, where facial recognition is introduced to

---

[101] Paul Mozur, Claire Fu & Amy Chang Chien, *How China's Police Used Phones and Faces to Track Protesters*, N.Y. TIMES (Dec. 2, 2022), perma.cc/KTM9-QF8U.

[102] *Id.*

[103] *Id.*; Ferguson, *supra* note 4, at 1198–99.

[104] Barrett, *supra* note 4, at 243.

[105] Steven Feldstein & David Wong, N*ew Technologies, New Problems – Troubling Surveillance Trends in America*, JUST SEC. (Aug. 6, 2020), perma.cc/MJ2L-Z85L ("Facial recognition-powered cameras in public squares can be used to quickly pull up a trove of personal information – citizenship, age, educational status, criminal history, employment, and even political affiliation – on individual citizens, without their knowledge.").

[106] Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1512 (2022) (citing Alice E. Marwick & Danah Boyd, *I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience*, 13 MEDIA & SOC'Y 114, 125 (2010)).

[107] Barrett, *supra* note 4, at 243; Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 388–91 (2008) ("At the core of the First Amendment is a commitment to the freedom of thought--recognized for centuries as the most vital of our liberties. In order to speak, it is necessary to have something to say, and the development of ideas and beliefs often takes place best in solitary contemplation or collaboration with a few trusted confidants . . . . If we are interested in a free and robust public debate we must safeguard its wellspring of private intellectual activity.").

[108] *See* Daniel E. Ho, Emily Black, Maneesh Agrawala & Li Fei-Fei, *Evaluating Facial Recognition Technology: A Protocol for Performance Assessment in New Domains*, 98 DENV. L. REV. 753 (2021).

investigate particularly egregious crimes and is slowly expanded to lower-level offenses.[109]

2. Inaccuracy and Inequities

Facial recognition also raises linked concerns about inaccuracy in the technology and inequities created by its use. First, accuracy: testing by the National Institute of Standards and Technology (NIST) has found that facial recognition's accuracy rates depend on the quality of the facial images being compared. Though accuracy rates are very high when facial recognition is applied to good-quality photos, low image quality and poor photography can cause problems.[110] A 2021 NIST study that tested twenty-nine facial recognition algorithms for verification of a traveler's face against a database of stored photos, for instance, showed a 99.5% or better accuracy rate.[111] Another NIST study, however, found that the error rates for one leading facial recognition algorithm jumped from 0.1% to 9.3% when applied to "wild photos," meaning photos that are not taken in controlled environments.[112]

Though the overall accuracy rate of facial recognition can be impressive under good conditions, its errors are not randomly distributed. In 2019, NIST found that false positives error rates are higher among certain demographic groups: West and East African, East Asian, Native American, American Indian, Alaskan Indian, and Pacific Islander.[113] It conducted a study that compared "189 software algorithms from 99 developers," which comprised the majority of the facial recognition industry at that time.[114] The study showed that "[u]sing the higher quality [] photos, false positive rates are highest in West and East African and East Asian people, and lowest in Eastern European individuals. This effect is generally large, with a factor of 100 more false positives between countries….With domestic law enforcement images [i.e., mugshots], the highest false positives are in American Indians, with elevated rates in African American and Asian populations; the relative ordering depends on sex and varies with algorithm."[115] In addition to discrepancies in how

---

[109] David Gray, *Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies*, 24 SMU SCI. & TECH. L. REV. 3, 47 (2021); *Mission Creep*, THEY ARE WATCHING, perma.cc/UWL6-WZUP (last visited Nov. 3, 2022).

[110] Grother et al., *supra* note 95.

[111] *NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding*, NIST (July 13, 2021), perma.cc/D65T-T7HF.

[112] William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does It Matter?*, CTR. FOR STRATEGIC & INT'L STUD. (Apr. 14, 2020), perma.cc/Q53H-29LG (citing NEC-002 FNMR at N=1.6M, R=1 on FRVT 2018 mugshots, and N=1.1M and R=1 on wild photos); Patrick Grother, Mei Ngan & Kayee Hanaoka, NISTIR 8280, Nat'l Inst. of Standards and Technology., *FRVT Part 2: Identification* (2020), perma.cc/U324-QZWF.

[113] Grother et al., *supra* note 95.

[114] Grother et al., *supra* note 95, at 1.

[115] *Id.* at 2.

the algorithms performed with respect to different ethnic groups, the study also found "false positives to be higher in women than men, and this is consistent across algorithms and datasets. This effect is smaller than that due to race."[116] Moreover, the study "found elevated false positives in the elderly and in children; the effects were larger in the oldest and youngest, and smallest in middle-aged adults."[117]

The discrepancy in facial recognition software performance across different races, genders, and ages is usually attributed to a lack of representation in the algorithms' training data. In fact, NIST tested the proposition that the location of a facial recognition algorithm developer can be a proxy for the training data that they used and found that "[a] number of algorithms developed in China give low false positive rates on East Asian faces, and sometimes these are lower than those with Caucasian faces."[118] Accordingly, NIST suggested that "training data, or perhaps some other factor intrinsic to the development, can be effective at reducing particular false positive differentials. Thus, the longer-term mitigation [for false positives] would be for developers to investigate the utility of more diverse, globally derived, training data."[119]

Disproportionate error rates across different demographics are concerning whether the errors are false positives (mistaken matches) or false negatives (mistaken lack of matches). False negatives can result in blocked and disrupted access. This was recently demonstrated by the inconvenience many ID.me users faced when trying to confirm their identities to obtain state government benefits.[120] False positives, on the other hand, can lead to false arrests.[121] In one notable 2020 case, the Detroit Police Department arrested Robert Julian-Borchak Williams, an African-American man, due to a false positive by its facial recognition system.[122] After a retail store reported a shoplifting, DPD detectives fed a blurry still image from a retail store surveillance camera into the state's facial recognition system.[123] One of the potential matches was Mr. Williams' driver's license photo.[124] During his later interrogation, Mr. Williams challenged the identification. Confronted with the live comparison of the security image and Mr. Williams' own face, Mr. Williams recalls an officer saying, "I guess the computer got it wrong."[125]

---

[116] *Id.*

[117] *Id.*

[118] *Id.* at 7.

[119] *Id.* at 71.

[120] Shawn Donnan & Dina Bass, *How Did ID.me Get Between You and Your Identity?*, BLOOMBERG (Jan. 20, 2022, 3:00 AM), perma.cc/27NL-YY88.

[121] Ferguson, *supra* note 4, at 1169.

[122] Hill, *supra* note 5.

[123] *Id.*

[124] *Id.*

[125] Melissa Nann Burke, *Michigan Man Wrongfully Accused with Facial Recognition Urges Congress to Act*, DETROIT NEWS (July 13, 2021, 10:04 AM), perma.cc/XMN8-YHFC.

Nevertheless, DPD refused to release him until "30 hours after being arrested."[126] Weeks later, at Mr. Williams' arraignment, the prosecutor moved to dismiss.[127] Unfortunately, Mr. Williams is not the only person who has been falsely arrested due to a false positive; at least two other Black men—Michael Oliver and Nijeer Parks—have also been wrongfully arrested based on a false positive match.[128] In Michael Oliver's case, the photo looked nothing like him, as even the judge agreed.[129]

These stories show both the dangers posed by false positive matches and the inadequacy of human verification as a safety measure. Scholars have pointed out that overreliance on technology, called automation bias, can be a major problem in law enforcement.[130] Automation bias is "the use of automation as a heuristic replacement for vigilant information seeking and processing,"[131] effectively treating the answer suggested by a computer program as a "trusted final answer."[132] Even though the facial recognition system used by DPD explicitly stated that the matches generated do not, by themselves, constitute a positive identification, DPD detectives failed to seek additional substantiating information aside from the retail store loss-prevention contractor's identification.[133] Police officers "in most jurisdictions [] do not appear to receive clear guidance about what additional evidence is needed to corroborate a possible face recognition match."[134] The lack of guidance and overreliance on technology is particularly concerning given the well-documented phenomenon that people tend to be poor at cross-racial

---

[126] *Id.*

[127] Hill, *supra* note 5.

[128] Elaisha Stokes, *Wrongful Arrest Exposes Racial Bias in Facial Recognition Technology*, CBS News (Nov. 19, 2020, 7:00 AM), https://perma.cc/J97C-76J3 (DPD arrested a man for an outstanding felony warrant after their facial recognition system rendered a false positive based on a still from a cell phone video); Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 6, 2021), https://perma.cc/2LAQ-RX33 (New Jersey police accused Nijeer Parks of shoplifting and attempting to hit a police officer with a car after a facial recognition system rendered a false positive based on the actual suspect's fraudulent driver's license).

[129] Stokes, *supra* note 129.

[130] *See* T.J. Benedict, Note, *The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest*, 79 WASH. & LEE L. REV. 849, 860 (2022) (discussing the risks associated with automation bias); Garvie et al., *supra* note 31 ("Companies and police departments largely rely on police officers to decide whether a candidate photo is in fact a match. Yet a recent study showed that, without specialized training, human users make the wrong decision about a match half the time.").

[131] Linda J. Skitka et al., *Automation Bias and Errors: Are Crews Better Than Individuals?*, 10 INT'L J. AVIATION PSYCHOLOGY 85, 86 (2000).

[132] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1271-72 (2008).

[133] Hill, *supra* note 5.

[134] Claire Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Geo. L. Ctr. on Priv. & Tech. (May 16, 2019), https://perma.cc/7B2X-JAEJ.

identification; humans are not a great check on these systems.[135] Considering other alarming reports of police departments failing to use high quality images and even using police sketches or photos of celebrities that purportedly look like a suspect, facial recognition's endemic issues of racial bias intermingle with undue trust in technology and the broader problems of lack of oversight and procedural safeguards around facial recognition.[136]

In addition to the possibility of false identification, many fear that the government will disproportionately apply facial recognition to minority populations that are already under increased government surveillance.[137] Professor Levendowksi has referred to the disproportionate application of facial recognition on certain minority communities as a form of "deployment bias."[138] The government's ability to make decisions about which areas or types of people are subject to facial recognition carries the threat of "[w]eaponizing surveillance technologies, such as face surveillance, against marginalized communities[,] render[ing] their movements hypervisible to law enforcement."[139]

Furthermore, even mere identification of some groups carries with it disproportionate impact. Through the use of facial recognition, the government could theoretically pull up an unknown individual's name and citizenship status at a glance.[140] This greatly facilitates policing of undocumented individuals and could shut them out of some public spaces. More generally, deployment bias may cause marginalized populations to feel the brunt of facial recognition's surveillance and free speech harms, deepening inequity within the United States.[141]

---

[135] *See* Bryan Scott Ryan, Note, *Alleviating Own-Race Bias in Cross-Racial Identifications*, 8 WASH. U. JURIS. REV. 115, 124 (2015).

[136] *Id.*

[137] *See, e.g.*, Amanda Levandowski, *Resisting Face Surveillance with Copyright Law*, 100 N.C. L. REV. 1015, 1030 (2022); Barrett, *supra* note 4, at 249.

[138] Levandowski, *supra* note 138, at 1029-30.

[139] *Id.*

[140] Feldstein & Wong, *supra* note 106 ("Facial recognition-powered cameras in public squares can be used to quickly pull up a trove of personal information – citizenship, age, educational status, criminal history, employment, and even political affiliation – on individual citizens, without their knowledge.").

[141] Civil liberties scholars have already identified deployment bias of facial recognition domestically and abroad. *See, e.g.*, *USA: Facial Recognition Technology Reinforcing Racist Stop-and-Frisk Policing in New York – New Research*, AMNESTY INT'L (Feb. 15, 2022), https://perma.cc/2G33-KXYB ("In the Bronx, Brooklyn and Queens, the research also showed that the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras."); Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://perma.cc/X73P-DYWB ("Chinese authorities already maintain a vast surveillance net, including tracking people's DNA, in the western region of Xinjiang, which many Uighurs call home . . . . The police are now using facial recognition technology to target Uighurs in wealthy eastern cities like Hangzhou and Wenzhou and across the coastal province of Fujian, said two of the people.").

These questions about racial bias are, in part, a symptom of a broader lack of oversight and auditing. A 2021 study found that among the 10% of police departments that claim to have facial recognition, only 15.8% of those claim to have a policy on facial recognition uses.[142] As emphasized by NIST's study of demographic effects on facial recognition, facial recognition algorithms are all different and, therefore, have different error rates.[143] A lack of oversight and auditing compounds the accuracy and racial bias concerns discussed above, as government agencies are not testing their facial recognition software's performance in general and across demographic groups.

This is a rapidly moving field. The NIST study on facial recognition accuracy was conducted in 2019. It is unknown what level of accuracy would be achieved were the study repeated in 2025 or, for that matter, were it done today. Even in 2018, the NIST chairman stated that the then-current test of facial recognition algorithms showed massive improvement from 2013—an only 5-year period.[144] But improved accuracy of algorithms would exacerbate, rather than eliminate, concerns about deployment bias and over-policing in minority communities.

3. Abuses by Individual Government Actors

In addition to contributing to concern about inequities, lack of oversight also carries the more specific risk that government actors may use the technology for personal and inappropriate purposes. In a 2016 Georgetown Center for Privacy and Technology report, the authors found that "major face recognition systems are not audited for misuse."[145] Especially considering that government entities and actors have access to much broader databases of facial images (such as driver's license databases, mugshot databases, etc.), a government employee could theoretically employ such systems to inappropriate or nefarious ends.

Existing databases and surveillance tools are abused with depressing regularity. Law enforcement officers have been accused of inappropriately using databases to stalk women in a number of states.[146] One particularly egregious episode involved a New York Police Department detective who hacked the phones of multiple people and also misused the federal National Crime Information Center to track the

---

[142] Oliver & Kugler, *supra* note 33, at 130–32.

[143] Grother, *supra* note 95, at 2.

[144] Charles H. Romine, *Facial Recognition Technology (FRT)*, NIST (Feb. 6, 2020), https://perma.cc/C4VB-53BC (statement of Dr. Charles H. Romine Director, Information Technology Laboratory, National Institute of Standards and Technology United States Department of Commerce).

[145] Garvie et al., *supra* note 31.

[146] AARON RIEKE ET. AL., CIVIL RIGHTS, BIG DATA, AND OUR ALGORITHMIC FUTURE 25 (Upturn 2014), https://perma.cc/U3MG-ZY22 (collecting cases).

communications of his ex-girlfriend, who was also a police officer.[147] There are also accounts, some confirmed by the agency, of National Security Agency employees passing around intercepted nude photographs and using surveillance tools to spy on former partners.[148] In addition to these salacious abuses, more mundane systems have also been misused. One key case under the Computer Fraud and Abuse Act concerned an IRS employee accessing the tax files of various political and personal opponents.[149] A similar case involved an employee of the Social Security Administration looking up current and prospective romantic partners, among others.[150]

Given the sheer size of the government bureaucracy, it is not surprising that there are some abuses. For example, the New York Police Department claims approximately 36,000 sworn officers and 19,000 civilian employees.[151] Some amount of misconduct is to be expected among such a large group. Hospitals and medical networks facing similar issues of personal privacy and scale are required to institute extensive safeguards to track employee use of patient files so that later auditing can detect inappropriate access.[152] Some incidents of government misconduct are known because of similar monitoring programs inside police departments and intelligence agencies. Yet facial recognition does not yet have a similar regime. Scary though it is to have a romantically obsessed individual access one's tax records, their being able to use facial recognition-enabled cameras to scan a city to find one's complete location history would be worse.

4. Data Security

Lastly, people have also expressed concern with the data security aspect of facial recognition.[153] Since everyone's face is unique, facial identity theft would be extremely difficult to ameliorate. Whereas someone might be able to request a new password if it were stolen, replacing one's face is not a viable—or desirable—solution for most.[154] However, it is not exactly clear whether facial recognition actually poses a data security threat that is so different in kind from the one created

---

[147] Dareh Gregorian & Ginger Adams Otis, *NYPD Detective Hacked into Computers to Get Fellow Officers' Email, Cell Phone Info: Feds*, N.Y. DAILY NEWS (May 21, 2013, 11:40 PM), https://perma.cc/28WA-QAHP.

[148] Cyrus Farivar, *Snowden: NSA Employees Routinely Pass Around Intercepted Nude Photos*, ARS TECHNICA (Jul. 17, 2014, 12:39 PM), https://perma.cc/37EU-JV94.

[149] United States v Czubinski, 106 F.3d 1069, 1071–72 (1st Cir. 1997).

[150] United States v. Rodriguez, 628 F.3d 1258, 1261–63 (11th Cir. 2010).

[151] City of N.Y., *About NYPD*, https://perma.cc/JF99-H3XK (last visited Jan. 31, 2023).

[152] *See, e.g.*, AuditBoard, *Understanding the HIPAA Audit Trail Requirements: Essentials for Compliance* (Nov. 17, 2021) https://perma.cc/3C9C-VFDB.

[153] *See, e.g.*, Candice N. Wright, Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections, U.S. GOV'T ACCOUNTABILITY OFF. (June 29, 2022), https://perma.cc/E389-Z5PN.

[154] *Id.*

by general availability of facial images. Most of the facial image data used in government facial recognition systems already exists in state databases. Moreover, it is unclear how the subsequent use of the stolen facial data would play out. Fooling a facial recognition security system with a false image of a face may be possible through the use of deepfakes,[155] or "videos that use machine-learning algorithms to digitally impose one person's face and voice onto videos of other people."[156] But were a hacker to seek to do that, they would presumably use a photo of a person's face rather than the hacked hash values stored by a facial recognition database to fool the system.

C. Current State of Facial Recognition Law and Line-Drawing Problems

The concerns with facial recognition outlined above do not apply with equal force to every government use of facial recognition. For example, use of facial recognition to verify government employees entering a government facility does not trigger the same ubiquitous surveillance concerns as deploying facial recognition to monitor live cameras across an entire city. And government authorities using facial recognition to scan a city for one missing child triggers fewer concerns than authorities using facial recognition to identify individual participants in a peaceful protest. A robust legal regime should account for these nuances.

The current legal regime largely leaves facial recognition unregulated, however. There are no federal laws addressing government use of facial recognition and, in general, the legal regime around facial recognition is lacking at the state and local level as well.[157] The lack of regulations around facial recognition has been particularly concerning in the law enforcement space, as there are currently no clear constraints on how the police can use this technology in most jurisdictions. Moreover, the regulatory void for facial recognition has left government actors without a clear benchmark for the kinds of information they should be collecting and assessments they should be conducting on their own facial recognition systems.[158]

Some have argued that the Fourth Amendment could be a means of constraining government use of facial recognition.[159] For example, Professor Andrew Ferguson

---

[155] Linda Rosencrance, *Privacy and Security Issues Associated with Facial Recognition Software*, TECHREPUBLIC (Aug. 25, 2022, 2:43 PM), https://perma.cc/WN66-6STY.

[156] Matthew B. Kugler & Carly Pace, *Deepfake Privacy: Attitudes and Regulation*, 116 NW. U. L. REV. 611, 613 (2021).

[157] Friedman, supra note 10.

[158] Wright, *supra* note 154, at 12–13.

[159] *See* Ferguson, *supra* note 4; Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591 (2017); Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO.

has suggested that Fourth Amendment jurisprudence incorporates several normative principles that are applicable to facial recognition to varying degrees.[160] Accordingly, law enforcement's use of facial recognition, Ferguson argues, could trigger the Fourth Amendment's procedural requirements.[161] Others are less convinced, however, and believe that current Fourth Amendment doctrine would not prevent government deployment of facial recognition.[162]

The major problem with using the Fourth Amendment to regulate facial recognition is that it is unclear whether government collection of facial data constitutes a Fourth Amendment "search." The Fourth Amendment provides procedural protections of the substantive right to be free from "unreasonable searches and seizures."[163] First, a court asks whether a given activity is a "search," and then it asks whether the search was reasonable. Since *United States v. Katz*, the Supreme Court has determined whether a "search" has occurred based on whether the government has violated a person's "reasonable expectation of privacy."[164] The Supreme Court in *United States v. Dionisio*, however, suggested that individuals do not have a "reasonable expectation of privacy" in their faces.[165] In isolation, this claim appears uncontroversial; your face is generally not a secret.

The lack of privacy in one's face does raise issues when combined with a parallel line of cases holding that it is generally permissible for the government to use video surveillance to monitor public spaces.[166] Though some courts are increasingly concerned about long-term public video surveillance—the First Circuit split evenly on this issue en-banc in 2022[167]—arguing that pervasive

---

MASON L. REV. 409 (2014); Matthew E. Cavanaugh, Note, *Somebody's Tracking Me: Applying Use Restrictions to Facial Recognition Tracking*, 105 MINN. L. REV. 2443 (2021).

[160] Ferguson, *supra* note 4, at 1132.

[161] *Id.* at 1141.

[162] Oliver & Kugler, *supra* note 33, at 113–15, 121–22; John Zens, Comment, *Face It: Only Congress Can Preserve Privacy from the Pervasive Use of Facial Recognition Technology by Police*, 58 SAN DIEGO L. REV. 143, 181–194 (2021); *see also* Sabrina A. Lochner, Note, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans*, 55 ARIZ. L. REV. 201, 214–216 (2013).

[163] U.S. CONST. amend. IV.

[164] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). For the centrality of the Harlan concurrence in subsequent understandings of the Katz holding, see Smith v. Maryland, 442 U.S. 735, 739-40 (1979).

[165] United States v. Dionisio, 410 U.S. 1, 14 (1973) ("No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.").

[166] *See, e.g.*, United States v. Houston, 813 F.3d 282, 287–88 (6th Cir. 2016), *cert. denied*, 580 U.S. 1021 (2016); *See also* Matthew B. Kugler & Thomas H. Rousse, *The Privacy Hierarchy: Trade Secret and Fourth Amendment Expectations*, 104 IOWA L. REV. 1223, 1277–79 (2019) (collecting cases).

[167] United States v. Moore-Bush, 36 F.4th 320 (1st Cir. 2022). Specifically, three judges would have overturned prior precedent permitting long-term pole camera surveillance and three

surveillance is different from isolated photography, it is far from a slam-dunk for privacy advocates. Facial recognition merely examines faces (which are public, entailing no Fourth Amendment violation) in video footage (which, if taken in public places, also entails no Fourth Amendment violation). Under current doctrine, then, it may well be that no use of facial recognition is a search.

Over the last several decades, however, the Supreme Court has recognized that emerging technologies raise independent surveillance concerns that may disrupt traditional conceptions of privacy. In the 1983 case *United States v. Knotts*, for example, the Supreme Court expressed its suspicion of sophisticated technology that could result in "dragnet type law enforcement practices."[168] Decades later, in *Carpenter v. United State*s, the Court reaffirmed this sentiment, holding that the police's use of historic cell-site location information to track an individual long-term violated their expectation of privacy.[169] Roberts, writing for the Court, stated, "[T]he time-stamped [cell phone location] data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[170] *Carpenter* suggests that the 2018 Supreme Court was amenable to considering the novel impact of surveillance technologies on its interpretation of one's "reasonable expectation of privacy." But the extent of the *Carpenter* revolution in Fourth Amendment law is unclear. The Supreme Court has not returned to the question since, and its membership has changed.

Even if privacy advocates persuade the Court to regulate facial recognition under the Fourth Amendment, the Court would immediately be faced with a line-drawing problem. In the context of criminal investigations, the government must generally get a warrant—or have a warrant-requirement exception—to conduct a search. But outside of the law enforcement context the rules are different. Under the special needs doctrine, the Fourth Amendment permits the government to conduct a search without a warrant under certain circumstances when the goal is not criminal law enforcement.[171] Specifically, the warrant requirement must be "impractical" in the given context and the search itself has to satisfy a reasonableness balancing test.

---

would not have overturned prior precedent. But the particular search at issue would be upheld under the good-faith exception regardless, so all were in agreement on the resolution of the particular case.

[168] United States v. Knotts, 460 U.S. 276, 284 (1983).

[169] Carpenter v. United States, 138 U.S. 2206, 2217 (2018).

[170] *Id.*

[171] *See, e.g.*, Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 444 (1990) (holding that stop at a DUI checkpoint is a seizure but is reasonable due to high government interest); *City of Indianapolis v. Edmond*, 531 U.S. 32, 48 (2000) (holding that states narcotics checkpoint was unconstitutional because primary purpose was criminal investigation and government interest was less immediate than in *Sitz*).

This category of special needs searches covers a diverse range of topics such as border and school searches and government personnel oversight.[172] Some of these use cases overlap with current and proposed uses of facial recognition, for instance airport customs and school security. Other proposed uses might also find themselves in this category. Take the example of the government using facial recognition in lieu of a patient check-in process at a public hospital. This is not a law enforcement activity and involves a context where people are already expected to verify their identities. It too might be permissible as a special needs search.

Some other proposed facial recognition uses might be analogous to a government checkpoint. Checkpoint stops do receive Fourth Amendment scrutiny, but they are sometimes permissible under the special needs doctrine. For example, the Supreme Court held in *Illinois v. Lidster* that an information-seeking checkpoint was constitutional because its primary purpose was not to detect crime but rather to solicit information about a past traffic accident.[173]

In fact, one could easily conceive of law enforcement using facial recognition in a situation similar to the facts of *Lidster* itself. In *Lidster,* law enforcement set up a highway checkpoint to identify witnesses to a prior hit-and-run.[174] Police—and even one criminal defense attorney—have used facial recognition to gather information on witnesses to crimes.[175] One could imagine using facial recognition to detect when an unidentified potential witness has returned to the scene of an incident. Using facial recognition to search a jurisdiction for a missing or dangerous person might also be assessed under the checkpoint cases. Those purposes, too, would not be "general crime control" and therefore would not automatically trigger a warrant requirement.[176]

Ultimately, however, all this doctrinal analysis is indeterminate. Both whether something is initially treated as a search and whether a special needs search is acceptable turn on the perceived reasonableness of the surveillance. Past work has argued that one way of assessing such reasonableness is investigating the public attitudes of everyday people.[177] To the extent that people view something as highly intrusive, then it makes sense for courts to view it as less reasonable. Similarly,

---

[172] *See* Kugler & Oliver, *supra* note 22, at 912 ("Noting that special needs cases span many different topics—from border searches to public schooling to government personnel management.").

[173] Illinois v. Lidster, 540 U.S. 419, 427 (2004).

[174] *Id.* at 422.

[175] *See* Valentino-DeVries, *supra* note 34 ("The sheriff's office said the technology was also sometimes used to help identify witnesses."); Kashmir Hill, *Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands,* N.Y. TIMES (Sept. 18, 2022), https://perma.cc/9ZDM-RGCW.

[176] *City of Indianapolis v. Edmond*, 531 U.S. 32, 47 (2000).

[177] *See* Kugler & Oliver, *supra* note 22, at 912; Kugler & Strahilevitz, *supra* note 19, at 224-244. Slobogin & Schumacher, *supra* note 20, at 737. Scott-Hayward, Fradella & Fischer, *supra* note 21, at 45-58.

public attitudes inform the democratic process. As elected officials seek to regulate facial recognition, they need guidance on what their constituents want.

Based on the concerns outlined in I.B, scholars can guess at what kinds of government uses of facial recognition might be most worrisome or offensive. But, without empirical evidence, they may not accurately reflect the actual privacy attitudes and expectations of ordinary people. Existing literature has already demonstrated that the public's comfort with facial recognition is highly context-specific,[178] suggesting that there will not be easy answers here. It is not known, for example, whether people believe that mere identification of a criminal suspect is more acceptable than scanning live feeds for them city-wide—or whether people believe it is acceptable for the government to scan airports and similar places to exclude unwanted individuals, as some private venues do.[179] A study that explores what kinds of uses the public will tolerate and support may provide useful, nuanced insights into the kinds of contexts that make ordinary people more or less comfortable with facial recognition. This kind of data could clarify what kinds of government uses, in what kinds of settings, are likely to be supported or rejected by the public.

III. EXAMINING PUBLIC ATTITUDES TOWARD GOVERNMENT USE OF FACIAL RECOGNITION

There are two basic questions for the regulation of facial recognition: where should the line be drawn between permissible and impermissible governmental uses, and where is it currently drawn? Given the norms of democratic accountability, public attitudes are likely relevant to where the line should be drawn. Lawmakers and judges may not defer to public attitudes, but they should at least be aware of them and take them into account. And, under the Fourth Amendment's reasonableness requirement, public attitudes are also relevant to the question of where the line is currently drawn. If a court is attempting to decide if warrantless surveillance is reasonable, it is helpful to know whether 20% or 80% of people consider the information gathering an undue intrusion. We therefore need guidance on what is reasonable. We need this guidance to solve the doctrinal questions of special needs searches, and we need it to inform the democratic debate if, as seems inevitable, the question of facial recognition becomes a problem for legislatures.

Past work has shown that people have nuanced views of facial recognition, making it difficult to know what the public will think about some of the uses

---

[178] *See* notes 201–03 and accompanying text; Matthew Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107 (2019).

[179] Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. TIMES (Dec. 22, 2022), https://perma.cc/WPW7-KXW6 (noting both the titular use by Madison Square Garden as well as retailers use of facial recognition against shoplifters).

currently under consideration. For example, survey research by Professor Sarah Katsanis and colleagues has shown that it matters a great deal what kind of entity is using facial recognition. Advertisers and foreign governments are among the least trusted entities and healthcare workers and researchers are among the most trusted entities. State and federal governments are in the middle, though law enforcement is actually more trusted than government in general.[180] Even within the relatively trusted medical space, however, it matters what facial recognition is being used for.[181] Similarly, my own past survey research has shown that people's comfort with regular businesses using facial recognition varies drastically depending on the business' aim.[182] For example, more people are comfortable than not with a store using facial recognition to detect known shoplifters (58.9%), but comparatively few are comfortable with stores using it for targeted advertising (25.8%). And a performance venue using facial recognition to detect a performer's known stalkers is rated as comfortable by a majority of respondents (60.0%), but a homeowner's association monitoring its own streets and sidewalks is not (31.9%).

Taken as a whole, this research shows that people's comfort with facial recognition is not simply a matter of some entities being trusted and others not, or some places being private and others not. There is a complex interplay between purpose and entity. And the government has unique purposes, unique powers, and a unique role in modern society. It is hard to know how it, and its goals, will be viewed by the public in this context.

Because of this uncertainty, novel data were needed. I therefore conducted a survey that asked people to rate their level of comfort with a variety of government uses of facial recognition. Participants evaluated scenarios drawn from both the set of current U.S. governmental uses as well as uses proposed or implemented in foreign countries. Broadly, there were three types of scenarios: ones concerning general identity verification and identification, ones addressing identification specifically in the law enforcement context, and ones in which facial recognition was conducted on live video feeds to identify passersby.

The survey was conducted in October 2022 using the Qualtrics survey platform and a sample provided by Dynata, an online survey firm with an established panel of respondents.[183] The demographics of the sample were set to match the proportions found in the U.S. Census on the dimensions of age, sex, region, education, race, and ethnicity. Full demographics are reported in Appendix A. The

---

[180] Sara H. Katsanis et al., *U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics*, 3 IEEE TRANSACTIONS ON TECH. & SOC., no. 1, 2022, at 9, 12–13, https://perma.cc/6Z9J-Q7JY.

[181] Katsanis et al., *supra* note 86, at 6 (discussing survey results that showed different levels of comfort across use type).

[182] Kugler, *supra* note 179, at 140.

[183] DYNATA, PANEL BOOK 5–6 (2020), https://perma.cc/3J5D-PVB8.

final sample contained 958 individuals.[184] Respondents received an email from Dynata inviting them to participate in the survey. If they clicked on the provided link, then they were routed to a Qualtrics survey hosted by Northwestern University. By monitoring the demographics of those completing the survey, Dynata targeted waves of survey invitations to create a final sample consistent with the desired quotas.

The main portion of the study asked participants to rate their level of comfort, on a 1 to 4 scale (Very Uncomfortable, Somewhat Uncomfortable, Somewhat Comfortable, Very Comfortable), with different government uses of facial recognition. The choice of "comfort" as the object of interest was intentional. Though it does not mirror the language of Fourth Amendment doctrine (violating reasonable expectations of privacy, being intrusive), it is the kind of term that everyday people readily understand. It also permits for an easily understood binary: people are either more comfortable than not or more uncomfortable than not. Since the goal here was to inform policy, language that was closer to preference-tracking seemed more appropriate.

The participants rated the fifteen total use cases in random order, with each appearing on the screen in isolation. The full text of these scenarios, along with the starting instructions, is in Appendix B. Though the below discussion breaks the use cases into the three categories described above (general, law enforcement, and live monitoring), participants were neither given those labels nor received the scenarios in those blocks. Following these ratings, participants made three forced choices regarding uses of biometrics and completed an attitudinal scale.

Primary analyses for these results took the form of a series of Analysis of Variance (ANOVA) tests. ANOVAs test whether scores from two or more samples differ systematically enough that the samples are likely to be statistically distinct. Comparisons between the different scenarios here—such as the use at customs and the use at the show in the public park—were within-subject: the same people rated each of these.

As described above, there was reason to expect a large amount of context-sensitivity in these ratings. This means that people would be expected to rate these facial recognition uses differently, rather than having a particular comfort level that applied to all government uses. I therefore began by testing whether there were

---

[184] Inattentive participants were screened from the final sample based on two criteria. First, participants who did not give the appropriate response to an attention-check question—a question asking participants to give a particular response—or a CAPTCHA item were unable to complete the study. Second, participants were screened from the final sample if they finished the study in less than one-third of the time taken by the median participant or if they wrote gibberish in a comment box. Of the participants who completed the study, 4.2% were screened on the basis of time or gibberish. For a discussion of attention checks in legal surveys, *see* Matthew B. Kugler & R. Charles Henn, *Internet Surveys in Trademark Cases: Benefits, Challenges, and Solutions*, *in* TRADEMARK AND DECEPTIVE ADVERTISING SURVEYS 291, 300–307 (Shari Seidman Diamond & Jerre B. Swann eds., 2d ed. 2022).

differences within each of the scenario categories and then moved to considering differences between categories.

A. Degree of Comfort with Different Governmental Uses of Facial Recognition (Study 1)

As can be seen in Table 1, the level of comfort with the general identification and verification uses varied substantially depending on context and purpose. Over 75% of participants were comfortable with using facial recognition to identify people at airport customs or to put a name to an unconscious patient at a public hospital. And 72% were comfortable with using facial recognition to verify the identities of people entering a high school. But this does not indicate a general comfort with all use of facial recognition. Under 40%, a minority, were comfortable with three other governmental uses. These three uses all concerned people being in public places: watching a show in a public park, attending a political rally, or walking into a building that hosted a support group meeting. Despite the public settings, more people were uncomfortable with these uses than were comfortable.

Two of the disfavored uses presented obvious freedom of association issues without countervailing government interest. The scenarios did not give the city government (the stated surveilling authority in these cases) a reason to want to identify the people who attended the support group meeting or a political rally for the mayor's opponent, and the First Amendment issues are clear.

But one of the disapproved scenarios did not raise a direct chilling effect concern. In that vignette, people who attended a publicly-funded show in a city park were identified with facial recognition and then later sent donation requests and advertisements for future shows. This scenario resembles conventional targeted advertising, not political oppression. It even serves a potentially laudable goal—increasing awareness of and support for free public entertainment. Nevertheless, it made a majority of people uncomfortable. It seems like there is a difference between using facial recognition to control access to secured/limited admittance areas like schools and airports and using the same technology in otherwise open-access spaces like public parks.

Table 1: Comfort with use of facial recognition to identify people for various non-law enforcement purposes.[185]

	Means	Percent Uncomfortable	Percent Comfortable	Ratio of Comfortable to Uncomfortable
Monitoring attendees at an AA meeting	2.12a (1.10)	63.4%	36.6%	0.58
Mayor monitoring opponent's rally	2.13a (1.10)	61.2%	38.8%	0.63
Sending donation requests and ads to park show attendees	2.17a (1.08)	62.8%	37.2%	0.59
Checking in patients at public hospital	2.67b (1.00)	41.3%	58.7%	1.42
Screening, public high school	2.98c (0.98)	27.8%	72.2%	2.60
Verifying identities at customs	3.09d (0.92)	22.2%	77.8%	3.50
Pub. hospital IDing unconscious patient	3.16d (0.88)	19.7%	80.3%	4.07

Note: Means are on a 1-4 scale, with higher numbers indicating greater comfort. Standard deviations are reported in parentheses. Means not sharing subscripts are significantly different at the $p < .001$ level.[186] The percent comfortable column combines the "somewhat" and "very" comfortable responses, and similarly for percent uncomfortable.

Moving on to law enforcement uses, four scenarios were crafted to reflect potential uses in police investigations. For one of these, facial recognition was used to identify a homicide suspect by searching for their image in the state driver's license database. As can be seen in Table 2, over 78% of participants were comfortable with that use. People were slightly less comfortable with using facial recognition to identify a car thief, but still almost 72% were more comfortable than not. Identifying a witness to a homicide made participants slightly less comfortable than the prior case, but again there was still strong support (62.9%). These three scenarios all described the crimes occurring in the same type of location—outside a bodega—so people should have been imaging scenes that were all equally public. Finally, the last scenario, with which only a minority of participants were comfortable, described a jaywalking traffic camera system, where violators were mailed tickets imposing fines.

These scenarios were intended to represent a range of possible investigatory uses. People were plainly comfortable with using facial recognition to identify perpetrators of serious crimes. But there was a drop-off between murder and nonviolent auto theft, and a substantial drop-off between a murder suspect and a witness to the same crime. Further, a majority was uncomfortable with using facial

[185] $F(4.02, 3848) = 358.21$, $p < .001$, $\eta^2 = .272$. Mauchly's W = .376 significant at $p < .001$, so Greenhouse Geisser correction used.

[186] The means for the first three scenarios do not differ at any significance level (all ps > .10). The means for the final two scenarios differ at $p = .012$.

recognition for the broadest of law enforcement purposes—basic traffic enforcement.[187]

Table 2: Comfort with use of facial recognition to identify people of law enforcement interest, depending on the crime and target.[188]

	Means		Percent Uncomfortable	Percent Comfortable	Ratio of Comfortable to Uncomfortable
Jaywalker traffic cam. System, ID	2.24	(1.08)	58.8%	41.2%	0.70
Witness to homicide, ID	2.77	(0.95)	37.1%	62.9%	1.70
Car thief ID, nonviolent	2.96	(0.94)	28.2%	71.8%	2.55
Homicide suspect, ID	3.13	(0.91)	21.7%	78.3%	3.61

Note: Means are on a 1-4 scale, with higher numbers indicating greater comfort. Standard deviations are reported in parentheses. All means in this table are significantly different than each other at the $p < .001$ level. The percent comfortable column combines the "somewhat" and "very" comfortable responses, and similarly for percent uncomfortable.

The final set of scenarios considered live facial recognition surveillance. As discussed above, the prospect of the government being able to scan a facility or a city to locate a particular individual using facial recognition is deeply worrying to some scholars.[189] Here there were four scenarios. Two of these vignettes described city-wide searches, one for a missing child and one for the same type of non-violent auto thief described in the previous set. These scenarios made clear the wide extent of the search. Consider the auto thief version:

A detective uses facial recognition technology to scan all public cameras in a city to locate a person suspected of stealing a car that had been parked overnight outside a bodega. The software compares the image from a bodega security camera to a live feed of all city owned cameras, including those on public buses, in public parks, and on street corners. When a match is found, the detective is notified of the suspect's real-time location.

Nevertheless, almost 70% of people were comfortable with the city-wide auto thief search (see Table 3). And over 80% were comfortable with the city-wide search for a missing child. People were similarly comfortable (77.6%) with TSA searching live camera feeds at an airport to look for known security threats. In sharp contrast to these, only 53.9%—a bare majority—were comfortable with using facial recognition to search a crowd watching a marathon for people with outstanding warrants.

---

[187] The jaywalking fine system may sound absurd, but it is simply an extension of the model currently used to monitor automobiles in some school zones and construction zones.

[188] $F(2.44, 2335) = 294.81$, $p < .001$, $\eta^2 = .236$. Mauchly's W = .727 significant at $p < .001$, so Greenhouse Geisser correction used.

[189] *See supra* Part I.B.

Table 3: Comfort with live facial recognition surveillance depending on its purpose.[190]

	Means		Percent Uncomfortable	Percent Comfortable	Ratio of Comfortable to Uncomfortable
Marathon Crowd Search, Warrants	2.57	(1.06)	46.1%	53.9%	1.17
City Search, Auto Thief	2.87	(0.97)	31.5%	68.5%	2.17
Airport Search, Threats	3.14	(0.93)	22.4%	77.6%	3.46
City Search, Missing Child	3.24	(0.92)	18.5%	81.5%	4.41

Note: Means are on a 1-4 scale, with higher numbers indicating greater comfort. Standard deviations are reported in parentheses. All means in this table are significantly different than each other at the $p < .001$ level. The percent comfortable column combines the "somewhat" and "very" comfortable responses, and similarly for percent uncomfortable.

The two auto theft cases—the identification of the static photo and the live search for the suspect's location—were compared. The crime was described identically in each case, so any difference between the comfort levels should reflect only the surveillance technique used rather than any other factor. And the surveillance technique was described very clearly, with the detective getting the suspect's name in one case and their real-time location in the other. Here, people were reliably more comfortable with the identification of the static image than with the live search, but the difference was quite small.[191] As can be seen by comparing Tables 2 and 3, there is only a 3.3 percentage point difference between the two comfort scores (71.8%-68.5%).

1. There Were Few Individual Differences in Comfort Levels

One prominent question in the facial recognition debate is the treatment of minority groups.[192] Algorithms have tended to be less accurate when assessing women and members of racial minority groups, and it is theorized that racial minorities in particular might be burdened by increased use of facial recognition by law enforcement.[193] It would therefore be concerning from an equity standpoint if racial minority groups and women were systematically less comfortable with government use of facial recognition and their views were obscured when aggregated with those of others.

To examine the role of race and gender in this study, a single composite score was created by averaging the comfort ratings from the individual scenarios. Since these ratings correlated well with each other, the composite showed high statistical

[190] $F(2.65, 2532) = 194.45$, $p < .001$, $\eta^2 = .169$. Mauchly's $W = .833$, which is significant at $p < .001$. Greenhouse Geisser correction used.

[191] A within-subjects ANOVA was conducted comparing just those two scenarios. The test was significant $F(1, 957) = 14.06$, $p < .001$ $\eta^2 = .014$. The means are as reported in Tables 2 and 3.

[192] *See* Part I.B.ii

[193] *Id.*

reliability.[194] A multiple regression was then conducted using that average comfort rating as a dependent measure and a variety of demographics as predictor variables. Many of the usual demographics were not helpful in predicting facial recognition attitudes. In Model 1, which contains race, ethnicity, gender (coded as female versus not), education, and region, only region and educational attainment were significant predictors. Those higher in educational attainment were more comfortable with facial recognition, as were those in the Northeast (compared to those in the Midwest).

Table 4: Standardized coefficients from a regression predicting overall comfort with facial recognition use.

	Model 1 ($r^2 = .029$)	Model 2 ($r^2 = .040$)	Model 3 ($r^2 = .124$)
Female	0.023	0.020	0.017
Black	0.011	-0.003	0.002
Asian	-0.005	-0.007	-0.026
Age	-0.067	-0.074	-0.129 ***
Hispanic	-0.033	-0.044	-0.034
Education	0.124 ***	0.110 **	0.168 ***
South	0.054	0.057	0.044
West	-0.037	-0.036	-0.021
Northeast	0.098 *	0.096 *	0.091 *
Republican		0.071	0.006
Democratic		0.130 ***	0.137 ***
Authoritarianism			0.310 ***

Note: Numbers are standardized coefficients for each predictor variable. * represents coefficients that are significant at the $p < .05$ level, ** ones at the $p < .01$ level, and *** at the $p < .001$ level. The regional comparison category was the Midwest. The r^2 term is a measure of variance explained in each model.

Model 2 adds terms representing identification with the Republican and Democratic parties (as opposed to Independents and members of third parties). Interestingly, both Republicans and Democrats were more comfortable with facial recognition than were Independents, and the coefficient was significant for Democrats.

Model 3 adds the authoritarian submission scale designed by Professor John Duckitt and colleagues.[195] The social psychological theory of authoritarianism defines authoritarians as people who are especially willing to submit to authority,

---

[194] Cronbach's Alpha = .925.

[195] Items on this scale include "It's great that many young people today are prepared to defy authority" (reverse coded), and "What our country needs most is discipline, with everyone following our leaders in unity." The response scale ranged from 1 (strongly disagree) to 6 (strongly agree). Higher scores indicate stronger endorsement of authoritarian ideologies. *See* John Duckitt et al, *A Tripartite Approach to Right-Wing Authoritarianism: The Authoritarianism-Conservatism-Traditionalism Model*, 31 POL. PSYCH. 685–715 (2010).

who believe that it is particularly important to yield to traditional conventions and norms, and who are hostile and punitive toward those who question authority or who violate such conventions and norms.[196] The authoritarian submission scale is designed to measure the first of these impulses: the extent to which people think that authority should be respected and obeyed.[197] It has previously been shown to correlate with privacy attitudes in the context of law enforcement surveillance.[198] Here, it was a substantial positive predictor of comfort with government facial recognition use.

In none of the three models are the coefficients from Black, Asian, Hispanic, or female respondents significant. This suggests that comfort with facial recognition is not sharply divided across the lines of race and gender. In fact, the r-square termed value is exceedingly low even for that complete model, suggesting that demographics as a whole matter very little. This is also not a surprising null effect. Prior work on privacy expectations has shown that few individual differences—apart from authoritarianism—are reliably predictive.[199] And specifically there have not been prior effects of race, ethnicity or gender, though educational attainment and age are sometimes significant.[200] The regional effect—more comfort in the Northeast—may be meaningful if regulation at the state level is being considered, however. A regression conducted that looked only at comfort with the four law enforcement facial recognition scenarios shows the same overall pattern. Specifically, the effects of gender and race remained non-significant while there were effects from educational attainment and authoritarianism.[201]

2. Preferences Concerning Use of Facial Recognition Verification

The previous set of questions concerned whether one would be comfortable being subjected to—or being in a society where others were subjected to—certain types of facial recognition. But it did not ask whether people would ever actively choose facial recognition. The next set of questions presented participants with three forced choices. For these choices, participants were told that they had two

---

[196] *See* Bob Altemeyer, *The Other "Authoritarian Personality," in* 30 ADVANCES EXPERIMENTAL SOC. PSYCH. 47–92 (Mark Zanna ed., Elsevier 1998).

[197] *See* Duckitt et al., *supra* note 196.

[198] *See* Kugler & Strahilevitz, *supra* note 19, at 254.

[199] Matthew B. Kugler & Lior Jacob Strahilevitz, *Assessing the Empirical Upside of Personalized Criminal Procedure*, 86 U. CHI. L. REV. 489, 507 (2019) (finding that a model containing 16 individual difference predictors still only explained 5.8% of the variance in privacy expectations).

[200] *Id.*, *But see* Chao et al., supra note 21, at 310–312 (finding greater privacy sensitivity among African Americans in the law enforcement context, though also finding no effect of Hispanic ethnicity and small and mixed effects of gender).

[201] Results available from the author upon request.

ways of verifying their identity. One of those ways involved facial recognition, and one involved a domain-appropriate conventional alternative.

One of the scenarios concerned passing through customs upon returning to the United States from an international trip:

Imagine that you are flying back into the United States after traveling to another country. As you approach customs at the U.S. airport, you have two options. Which option do you take? Assume that you are traveling alone and not trying to make a connecting flight.

A. You can approach a computer terminal that will compare your face to the image on your passport. There are many terminals, and there are no lines.

B. You can wait in line for a person to compare your face to the image on your passport. The line for this option appears to be 25 minutes long.

The order of the facial recognition and non-facial recognition alternatives was counterbalanced, so half the time the facial recognition option came first and half the time it came second. Further, there were two variants for this airport case. One is as is printed above: a 25-minute wait for a human. The other said that there was no wait for a human. Half the participants received each of these variants.

As can be seen in Table 5, three-quarters of the sample opted for facial recognition when the alternative was a 25-minute wait for a human. Substantially fewer people, though still a majority, opted for facial recognition even when there was no wait, however.[202]

The other two scenarios did not have alternate versions; all participants got each of them. One of these concerned checking in for an appointment at a public hospital. Patients could either be identified with facial recognition, or by verbally confirming their information with a receptionist in the waiting room.[203] The other scenario concerned filing one's taxes online. Identity could be verified either with facial recognition or by typing in one's adjusted gross income from the previous year and driver's license number (twice).[204] For both of these scenarios, about a third of

---

[202] The two customs scenarios differ at $\chi^2(1) = 59.95$, $p < .001$, and both also differ from the other two (0 minute wait with tax $\chi^2(1)=14.24$, $p < .001$, hospital $\chi^2(1) = 32.40$, $p < .001$) (25 minute wait with tax $\chi^2(1)=15.30$, $p < .001$, hospital $\chi^2(1) = 12.85$, $p < .001$). The tax and hospital scenarios do not differ from each other $\chi^2(1) = 0.002$.

[203] Here is the full text:

Imagine you are a patient coming in for an appointment at a public hospital. To check in for your appointment, you have two options. Which do you choose?

A. Show your face to a computer that will use its camera and facial recognition to match your face to the image in your patient portal.

B. Approach the front desk and tell the receptionist your first and last name, and then verify your date of birth and the street that you live on to confirm your identity.

[204] Imagine you are filing your taxes on your home computer through a government website. As part of this process, you need to verify your identity several different ways. You have

participants opted for facial recognition and two thirds for the conventional alternative.

Table 5: Preference for biometric verification in a variety of contexts.

	Biometric	Other option
Customs check-in, with 0-minute wait for a human	53.5%	46.5%
Customs check-in, with 25-minute wait for a human	77.2%	22.8%
Hospital returning patient check in.	33.4%	66.6%
Tax filing identity verification	33.5%	66.5%

These data show that the comfort people often report with facial recognition does not amount to a preference for it. In contexts where people do not often use facial recognition, such as patient check in and tax filing, most would still prefer to not. But facial recognition has been used at airport customs for some time. About half of the sample would prefer biometric verification to human verification, even with no wait, and about half of the remaining people would opt for biometrics if it was faster. This suggests that there is some willingness to tolerate facial recognition in exchange for convenience. Notably, however, about a quarter of respondents are still resistant to facial recognition use, even in a highly non-private setting and even when resisting imposes a substantial cost in terms of wait time. It is possible that these participants are overstating their willingness to incur costs to protect privacy—some previous work has shown that people are more likely than they themselves would expect to accept privacy invasions.[205]

B. Comfort and Perceived Accuracy of Facial Recognition (Study 2)

In addition to its increasing prevalence, the other major change regarding facial recognition over the past decade has been its accuracy. As described in Part I.B.ii., facial recognition is now far more accurate than it once was. At the same time, there are still accuracy-related problems.

---

two options. Which option do you choose? Assume you have the required documents (driver's license and prior year's taxes) available.

A. Allow the government website to use your laptop camera. It will take an image of your face from several angles and compare it to your driver's license photo. If it detects a match, you can file without further verification. If it does not detect a match, you can enter your information as in the other option.

B. Enter into the government website all the information it requests. This will require you to enter your driver's license or passport number twice - once for federal, once for state - your date of birth, and last year's adjusted gross income (found on page 1 of last year's return).

[205] Roseanna Sommers & Vanessa Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 Yale L.J. 1962, 1985 (2019) (finding that almost all experimental participants were willing to unlock their phones and hand them to an experimenter upon request even though only a quarter of forecasting participants said they would have complied).

A follow-up study was therefore conducted to determine whether positive and negative information about the accuracy of facial recognition would substantially affect comfort with its use. A sample of American adults was recruited in January 2023 by CloudResearch. The demographics of the sample were set to match U.S. Census proportions on the dimensions of age and sex, but race, ethnicity, and educational attainment could freely vary. This produced a sample that was somewhat less Hispanic and somewhat more African American than in the first study, but was broadly similar. The sample was still politically neutral and neither more nor less educated than in Study 1. Full demographics are reported in Appendix A. The final sample contained 608 individuals.[206] The changes in sample size and provider were aimed at reducing the cost of the survey.

The procedure for this study mirrored that of the first. After completing the demographic questions, participants were randomly assigned to read one of three short descriptions of facial recognition. In the "works well" condition, the description said that facial recognition is highly accurate for good quality photos, and that a study by NIST has confirmed the increasing accuracy of it over time. In the "false negative" and "false positive" conditions, the descriptions said that algorithms still had trouble identifying people in low quality or uncontrolled photos, that there were particular problems identifying women and ethnic minorities, and that testing by NIST had shown continued issues with either false positives or false negatives. All of the statements in both conditions are factually correct. They simply focus on either the positive or negative points and omit the conflicting information. Participants were forced to spend twenty seconds on the page with this text and the text remained when the following two questions were displayed.

There were two checks on the manipulation. One was a question asking participants to select the answer that best represented the finding of the government study described in the manipulation. The answer choices reflected each of the three conditions (substantial improvements in accuracy, false negative problems, and false positive problems) and one alternative saying the study was inconclusive. This was intended to be a hard check—perhaps similar to an SAT reading comprehension question. In the "works well" condition, 73.6% of participants chose the correct answer. Fewer picked the correct answer in the two negative conditions (39.1% for false negative, 59.3% for false positive), generally because of confusion between the two types of negatives (over 70% picked one of the negative options in each of those conditions). The following analysis looks at both those who got the question right as well as those who got it wrong. Were the

[206] As in Study 1, a few participants were removed for being speeders or putting inappropriate responses to the free response comment box at the end of the study (8 participants). Participants were also unable to complete the study if they did not select the correct answer to an early question that asked them to select a particular response option.

analysis restricted to those who got the question right then the pattern of results would be unaffected.[207]

The other manipulation check asked participants to rate on a three-point scale how effective they believed facial recognition technology currently is. Participants thought that facial recognition worked better in the works-well condition than the other two, which did not differ.[208] In the works well condition, only 3% thought that facial recognition was "not very effective" compared to 24% and 26% in the false negative and false positive conditions, respectively. This suggests that the manipulation was successful in giving people different overall impressions of facial recognition.

To test the impact of this manipulation on views of facial recognition, five scenarios from Study 1 were selected that sampled the range of possible uses. As shown in Table 6 below, three of these uses (marathon search for outstanding warrants, airport search for threats, and city search for a missing child) use live facial recognition to surveil some subset of the populace. One is a straightforward use for law enforcement purposes: the identification of a car thief. And one is a convenience use: screening at the entrance of a public high school.

The pattern is the same for each of these uses. Comfort is higher in the "works well" condition than in the two conditions in which facial recognition is described as having problems.[209] In two of the five cases, false positives created more discomfort than did false negatives. But these differences were small, and people do not appear to be viewing false positive and false negative errors as drastically different. In general, the Study 1 results for these scenarios tend to fall between the "works well" condition and the two problem conditions.

---

[207] The significance of two of the many comparisons did shift, however. Specifically, the significance of the false positive-false negative distinction in the car thief case drops to p = 076, meaning it loses significance, and the difference between works well and false negative in the marathon case becomes significant .032.

[208] $F(2, 608) = 39.04$, $p < .001$, $\eta^2 = 0.114$. Works well ($M = 2.35$, $SD = 0.54$), False negative ($M = 1.88$, $SD = 0.59$), False positive ($M = 1.89$, $SD = 0.63$).

[209] High school, $F(2, 608) = 5.38$, $p < .001$, $\eta^2 = 0.017$.
Car thief, $F(2, 608) = 8.35$, $p = .005$, $\eta^2 = 0.027$.
Marathon, $F(2, 608) = 10.69$, $p < .001$, $\eta^2 = 0.034$.
Airport, $F(2, 608) = 8.21$, $p < .001$, $\eta^2 = 0.026$.
Missing child, $F(2, 608) = 5.86$, $p = .003$, $\eta^2 = 0.019$.

Table 6: Comfort with various uses of facial recognition technology as a function of accuracy manipulation.

	Mean ratings					
Scenario	Works Well		False Negative		False Positive	
Screening, public high school	3.01a	(0.91)	2.72b	(1.01)	2.71b	(1.03)
Car thief ID, nonviolent	3.04a	(0.84)	2.83b	(0.90)	2.67c	(0.94)
Marathon crowd search, warrants	2.72a	(0.99)	2.54a	(0.95)	2.27b	(0.98)
Airport search, threats	3.20a	(0.88)	2.89b	(0.96)	2.83b	(0.99)
City search, missing child	3.20a	(0.96)	2.97b	(0.95)	2.86b	(1.04)

	Percent Comfortable		
	Works Well	False Negative	False Positive
Screening, public high school	73.0%	62.7%	61.1%
Car thief ID, nonviolent	75.7%	69.2%	63.3%
Marathon crowd search, warrants	60.3%	54.2%	41.2%
Airport search, threats	81.0%	69.6%	64.8%
City search, missing child	79.9%	72.9%	69.0%

Note: Means are on a 1-4 scale, with higher numbers indicating greater comfort. Standard deviations are reported in parentheses. Means in each row not sharing subscripts are significantly different at the $p < .05$ level. The percent comfortable column combines the "somewhat" and "very" comfortable responses.

The modest size of these effects makes clear that people are not accepting facial recognition solely on the premise that it works with some magical level of accuracy. People are broadly comfortable with use for basic law enforcement purposes even when there is some chance of error. A greater chance of error, perhaps especially a greater chance of false positive error, lowers comfort levels. But, as can be seen in Table 6, the majority of people are still comfortable with most of these uses.

As mentioned before, there is considerable uncertainty about the exact efficiency of facial recognition technology today, and it is unknown how efficient it will be in the future. These data suggest that increasing accuracy should alleviate some of the discomfort with facial recognition. They also suggest that even persuading people that facial recognition is substantially flawed will not cause a wholesale rejection of its use.

C. Comfort with Prolonged Facial Recognition Monitoring (Study 3)

Though Study 1 considered a wide variety of uses of facial recognition, one topic it did not address was the ability to use facial recognition data to organize archival footage of a person. Much like the historical cell-site data at issue in

Carpenter, facial recognition has the power not just to identify a person or show where they are now, but also where they have been over time—to sift through the footage of a camera network for places and times where the person might appear.

A follow-up study was therefore conducted to determine whether people would differentiate between live surveillance of a person—finding where they are now—and this kind of archival search. A sample of American adults was recruited in August 2023 by CloudResearch. As in Study 2, the demographics of the sample were set to match U.S. Census proportions on the dimensions of age and sex, but race, ethnicity, and educational attainment could freely vary. The sample was more educated, less Hispanic, and more liberal than that of Study 1. Full demographics are reported in Appendix A. The final sample contained 642 individuals.[210]

The procedure for this study mirrored that of the first two. After completing the demographic questions, participants were randomly asked to rate surveillance scenarios that depicted either an investigation of a homicide or an auto theft. This was a between-participant factor, meaning that each person saw only one crime type or the other). For the given investigation, three uses of facial recognition were described. The detective was described as using facial recognition to identify a suspect's image from a store security camera, to find the real-time location of the suspect using a public camera system, or to scan the public camera system to find where the suspect had been over the prior week, with links to the archival footage.[211] This was a within-participant factor, meaning that each participant saw each of the three possible uses.

Given that this sample was less representative than that of Study 1, and particularly that it differed on political orientation, the base rates from Study 3 are likely less reflective of those from the general population. The cross-condition comparisons, however, should still be valid because people were randomly assigned to each condition. Here, we see a clear pattern. Participants were more comfortable with the use of facial recognition for identification than they were for

---

[210] As in Study 1, a few participants were removed for being speeders or putting inappropriate responses to the free response comment box at the end of the study (7 participants). Participants were also unable to complete the study if they did not select the correct answer to an early question that asked them to select a particular response option.

[211] The text of the archival search for the auto theft condition is presented below. The text of the first two scenarios was modified from the Study 1 versions to make it more parallel to this. In the homicide condition, the only changes were "investigating a murder. A man was killed outside a store…"

"A detective is investigating an auto theft. A car was stolen while it was parked overnight outside a store, and the store security camera caught an image of the suspect. The detective uses facial recognition technology to scan all public cameras in a city to find where the suspect has been over the prior week. The software compares the image from the store security camera to a live feed of all city owned cameras, including those on public buses, in public parks, and on street corners. When a match is found, the detective is given a map of the suspect's location over that week-long period, with links to the stored video footage."

finding a suspect's current location or doing historical tracking, but the latter two categories did not significantly differ.[212]

Table 7: Effect of using facial recognition to conduct a search of archival video data.

Scenario		Identification	Current Location	Historical Tracking (1 week)
Auto Theft	Mean	2.96 (0.98)	2.83 (1.00)	2.78 (1.01)
	% Comfortable	73.6%	67.7%	64.3%
Homicide	Mean	2.92 (0.98)	2.86 (0.99)	2.88 (0.97)
	% Comfortable	70.9%	65.6%	68.3%

Note: Means are on a 1-4 scale, with higher numbers indicating greater comfort. Standard deviations are reported in parentheses. The percent comfortable column combines the "somewhat" and "very" comfortable responses, and similarly for percent uncomfortable.

This form of duration neglect—not differentiating between finding the location of a person at a single point in time and finding their location over time—has been previously shown in the surveillance domain. Prior work shows that most people believe that tracking a person's GPS signal for a day, week, or month is equally violative of their privacy as using the signal to locate them at all.[213] Notably this does not mean that people viewed all as acceptable—most instead viewed them all as equally unacceptable. But the level of discomfort only slightly changed as the duration of surveillance increased, and most people chose the same response option for each.[214]

IV. A WAY FORWARD INFORMED BY PUBLIC ATTITUDES

The data show that people hold nuanced views of government facial recognition use. For non-law enforcement purposes, respondents were generally comfortable with the use of facial recognition for identification in secure spaces. Securing schools, monitoring airports, and presumably basic employee management would all fit into this category. However, the results clearly indicate that people were not comfortable with the use of facial recognition for general identification in all public spaces—even when used for facially legitimate purposes. Further, people were particularly uncomfortable about the use of facial recognition to identify people attending sensitive events, as in the campaign rally and alcoholics anonymous scenarios.

---

[212] A mixed ANOVA on the mean comfort ratings showed an effect of facial recognition type $F(1.83, 1171) = 7.28$, $p < .001$, $\eta^2 = 0.011$. Mauchly's $W = .909$ significant at $p < .001$, so Greenhouse Geisser correction used. Comparison of means showed that Identification ($M = 2.94$, $SD = 0.98$) was significantly higher ($p < .01$) than either current location ($M = 2.84$, $SD = .99$) or historical tracking ($M = 2.83$, $SD = .99$), which did not differ ($p = .65$). There was no interaction between facial recognition type and crime type.

[213] Kugler & Strahilevitz, *supra* note 19, at 246–249.

[214] *Id.* at 249.

For law enforcement uses, people's comfort levels seemed to be dependent on the nature of the crime. The results suggest that people are most comfortable with the use of facial recognition for the investigation of serious crimes and are resistant to it being used as a tool for minor quality-of-life offenses. Notably, people were only slightly less comfortable with the use of live scanning—actively searching a city's feed for a suspect's location—compared to identification of an image. Even pulling historic location information by scanning archival data only made people somewhat less comfortable than mere identification. Overall, people were generally quite comfortable with some of these more ambitious uses. And this comfort did not depend on the gender or race of the respondent; there were no significant effects on either of those factors. So this is not a case of a white racial majority imposing its differing privacy preferences on objecting minority groups.

In addition to being more comfortable with live scanning and archival searching than might have been expected, people were also less concerned about inaccuracy. Even when confronted with biased information about the accuracy of facial recognition in Study 2, most people were still comfortable with most uses. So the level of comfort observed in Study 1 is not based upon some unrealistically optimistic view of facial recognition effectiveness.

Some have described the battle over facial recognition as a conflict between those inclined to trust the government (and law enforcement) by default and those who view all law enforcement surveillance as a trap, a means of further inequality and oppression.[215] Most people, however, do not fall into either camp. They seek a middle ground, allowing for some uses while prohibiting others. If a government wishes to channel the views of the governed, it should account for this, at least to some degree.

Yet, in all of this, a sizable minority is uncomfortable. About a quarter of the people in Study 1 report being willing to wait in line for twenty-five minutes to avoid using facial recognition at the airport. And many people, particularly in the low-accuracy conditions of Study 2, report discomfort with uses that have majority support.

There is also a theoretical justification for erring on the side of increased privacy protection. Professor Anita Allen argued that privacy is a "precondition of a liberal egalitarian society" as opposed to "an optional good."[216] Privacy permits individuals to explore and experiment with different identities and "to engage in meaningful reflection, conversation, and debate about the grounds for embracing, escaping, and modifying particular identities."[217] Overall, these opportunities promote liberalism and democracy. That a majority is willing to sacrifice some amount of privacy does not mean that it is good for society to allow it to do so.

---

[215] *See* Ferguson, *supra* note 17, at 214-220, 230–234.

[216] Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 740 (1999).

[217] *Id.* at 755–56.

Applying Professor Allen's theory of privacy to government use of facial recognition technology would likely result in treating comfort levels as a floor for privacy protection rather than a target. So the government should not engage in uses with which a majority is uncomfortable, but it should not, conversely, be free to engage in all uses with which a majority of people are comfortable. Rather we should consider the cumulative effect that personal losses of privacy—despite public approval of such losses—may have on democracy. Thus, the below proposal considers not just public attitudes but also this democratic concern.

The below recommendations recommendation draws on a prior proposal made by Professor Andrew Ferguson and a proposal created by Professors Clare Garvie, Alvaro Bedoya, and Jonathan Frankle of the Georgetown Law Center on Privacy and Technology.[218] Professor Ferguson's legislative recommendations center predominantly on the distinctions between the different kinds of facial recognition techniques: face verification (confirming that a person matches the provided digital image),[219] face identification (searching through a database of faces to identify a particular person),[220] face tracking (following a particular person on stored or live video using their face),[221] and face surveillance (generalized monitoring of public spaces using a pre-populated list of faces).[222] Accordingly, Professor Ferguson recommends the following legislative solutions: (1) "ban generalized face surveillance" "with the only exceptions being for emergency or non-law enforcement uses;"[223] (2) "require a probable cause warrant for face identification;"[224] (3) "ban or require a probable-cause plus standard (akin to the Wiretap Act) for face tracking;"[225] and (4) "limit face verification to international border crossings."[226]

The Center on Privacy and Technology proposal is somewhat similar. It would require a warrant for law enforcement use of face identification and restrict this use to a defined set of crimes.[227] It would also sharply restrict any use of live facial tracking to only the most extreme and limited of circumstances.[228] Both this proposal and that of Professor Ferguson, however, are focused on law enforcement's use of facial recognition rather than all governmental uses. They also

---

[218] *See* Ferguson, *supra* note 4, at 1197; Garvie, Bedoya & Frankle, *supra* note 31 archived at https://perma.cc/U2GY-JL5U.

[219] *See* Ferguson, *supra* note 4, at 1113.

[220] *Id.* at 1114.

[221] *Id.* at 1122.

[222] *Id.* at 1116.

[223] *Id.* at 1197–99.

[224] *Id.* at 1199–1202.

[225] *Id.* at 1202–05.

[226] *Id.* at 1205–07.

[227] Garvie, Bedoya & Frankle, *supra* note 31 at https://perma.cc/U2GY-JL5U, recommendations 4 and 5.

[228] *Id.*, recommendation 6.

both did not have the benefit of this empirical evidence. I will discuss distinctions between these proposals and my own statutory recommendations below.

A. Non-Law Enforcement Use of Facial Recognition

As discussed in Part 1.C, many governmental non-law enforcement uses of facial recognition would likely be subject to a special needs search analysis under the Fourth Amendment. When "special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable,"[229] that requirement may be relaxed. In such circumstances, courts conduct a balancing test that weighs the strength of the government interest against the intrusion on individual liberty.[230] Generally, courts have assessed reasonableness by looking at "the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty."[231]

The data derived from these studies might help inform a potential special needs analysis for non-law enforcement uses of facial recognition technology. A court could use the fact that respondents expressed discomfort with facial recognition being used for the purpose of general identification as a factor in evaluating reasonableness. In particular, this discomfort with general identification could inform or affect an assessment of the "the severity of the interference with individual liberty."[232]

Take the scenario wherein respondents were asked to rate their comfort with a city park sending donation requests and advertisements to the attendees of a show in said public park. Unlike the scenario in which the mayoral candidate used facial recognition to identify attendees of an opponent's campaign, nefarious motivations are absent from the park situation. In contrast to the scenario wherein facial recognition was used to identify attendees of an AA meeting (as they entered from public streets), there is no obvious chilling effect here either. Despite these key distinctions, barely a third of the sample was comfortable with the use of facial recognition in this generalized manner. Accordingly, the data suggest that even though seeking park donations may "advance the public interest" under the reasonableness balancing test, the public's discomfort may outweigh that government interest.

Conversely, respondents generally indicated comfort with the use of facial recognition in secure areas, such as airports, or areas where one is already likely to

---

[229] *See, e.g.*, Skinner v. Railway Lab. Execs. Ass'n, 489 U.S. 602, 619 (1989); City of Ontario v. Quon, 560 U.S. 746, 756 (2010).

[230] *See, e.g.*, *Skinner*, 489 U.S. at 619.

[231] Illinois v. Lidster, 540 U.S. 419, 427 (2004) (citing Brown v. Texas, 443 U.S. 47, 51 (1979)).

[232] *Id.*

be asked for identification, such as a hospital. Respondents' higher comfort levels with access-specific verification, as opposed to more generalized identification, suggest that "the interference with individual liberty" in these scenarios is perceived as less severe. Accordingly, access-specific verification may be more reasonable under a special needs balancing test.

Finally, consider the live tracking cases. Use of facial recognition to look for high-risk people at an airport or search a city for a missing child is not "general crime control" and therefore may be evaluated under a special needs analysis.[233] People's apparent comfort with those highly limited uses should also be accounted for in the special needs analysis.

In all of these cases, however, the comfort of the public is only one relevant factor. The interest of the government differs in each scenario and the efficacy of facial recognition in promoting that interest also varies. So, it is not as simple as "comfort above this point is legal, and comfort below it is not." Consider the example of facial recognition in schools. People are broadly comfortable with the idea of using facial recognition in school security and access control. But that does not end the conversation of whether it is constitutional. A court should consider how well the system works in practice, whether inaccuracies are particularly burdensome to some group(s), and whether the system actually furthers a government interest. Any of those details might shift the special needs reasonableness analysis.

A statute informed by public comfort levels could use the general distinction between identity verification and general identification as a broad guideline for permissible versus impermissible non-law enforcement uses of facial recognition. Broadly speaking, such a statute could treat the use of facial recognition as permissible in three instances:

First, under a statute based on public attitudes, facial recognition would be permissible in circumstances where the government already demands identification or predicates access upon identification. For example, it would be permissible for the government to use facial recognition for identity verification purposes in airports as a means of facilitating the passport check process or the security check-in process. Here, the public attitudes approach would allow substantially more facial recognition use than Ferguson's proposal.[234]

Second, under such a statute, it would be permissible for the government to use facial recognition to scan for security risks within government buildings and similar installations—including schools. But the scope of this scanning should be limited. There should be a sharp differentiation between scanning for people expected to be a threat to that facility—e.g., a person on a no-fly list in an airport—and a person

---

[233] City of Indianapolis v. Edmond, 531 U.S. 32, 47 (2000).

[234] Ferguson, *supra* note 4, at 1205–07.

only of general interest to the government—e.g., a person in a gang database at a public hospital).

Third, facial recognition would also be permissible for security purposes at major events. There will be times when the kind of public space that normally should not be subject to facial recognition monitoring will temporarily be host to the kind of event that would benefit from extra monitoring or security. Consider parades, marathons, and concerts. But any use of facial recognition at such events must again be sharply limited in scope. General crime control objectives, such as the serving of warrants, should not be permissible under this non-law enforcement objective, nor should less-urgent government purposes, such as attendance tracking. The government would also not be permitted to use facial recognition to retrospectively identify people at these gatherings except as part of a criminal investigation, as described in the next section.

Conversely, it would not be permissible for the government to use facial recognition for general monitoring of the public on public streets or in public places such as parks, except as part of an authorized criminal investigation or in an emergency setting, both described in the next section. So it would not be legal for a government official to ask the system to "find Bob" and have it scan the public streets and public transit for Bob.

Finally, a statute should require disclosure of the existence and general parameters of the facial recognition system whenever it is added to a government facility or deployed for an event. If the public does not have notice of a system, then the democratic process cannot effectively regulate it. Not all facial recognition systems are alike, and many have varying error rates.[235] This heightens the need for public information; there is much worth knowing about any particular facial recognition system. And any system should have an audit trail so that abuses can be detected and investigated.[236]

B. Law Enforcement Use of Facial Recognition

The Fourth Amendment's warrant requirement generally functions as an on-off switch. In the criminal investigation context, if something is a search then a warrant based upon probable cause—or an exception to the requirement—is needed.[237] If something is not a search, then a warrant is not needed. The severity of the crime and the availability of alternative investigatory methods are not constitutionally

---

[235] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, *supra* note 95 ("Different algorithms perform differently.").

[236] For more discussion of how record keeping and auditing could work, see Garvie, Bedoya & Frankle, *supra* note 31 at https://perma.cc/U2GY-JL5U, https://perma.cc/C9KV-EXS4.

[237] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("[W]arrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing.").

relevant,[238] and there is not a "sometimes a search" alternative. Public attitudes, however, care a great deal about crime severity in this context. To approximate in policy what public attitudes suggest, a statutory solution is needed. I therefore propose a tiered approach, akin to the Wiretap Act, for addressing law enforcement uses of facial recognition that incorporates public attitudes to reflect varying levels of comfort with facial recognition.

The studies indicate that the crime at issue is a significant factor in public comfort levels. The importance placed on the crime being investigated is reflected in the difference in comfort scores between the scenario in which facial recognition is used to identify a homicide suspect and the scenario in which facial recognition is used to identify a jaywalker. The difference amounts to 37.1%.[239] Clearly, respondents were uncomfortable with the use of facial recognition for investigating non-serious crimes. Some participants were even made uncomfortable by changing the crime from murder to auto-theft, though a majority were still comfortable.

I therefore propose that use of facial recognition should only be permitted for serious crimes. The Wiretap Act can be a model here. As with public attitudes, the Wiretap Act is not transsubstantive: different crimes have different rules. It creates additional procedures—beyond standard Fourth Amendment requirements—for wiretapping. Under the Act, government actors seeking to wiretap as a means of gathering evidence must obtain a superwarrant, demonstrate that they are using wiretapping only to investigate a limited set of crimes (which includes most felonies),[240] and that other alternatives have been exhausted or are unlikely to succeed.[241] Additionally, only certain officials can sign applications for a Wiretap Act warrant,[242] and the wiretapping is subject to a minimization requirement[243] and continuing review.[244] The Wiretap Act can be understood as Congress' recognition that wiretapping raises heightened privacy concerns and that government use of wiretapping should only be used for particular crimes, for a limited set of time, and only after additional procedures have been followed.

---

[238] William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 847 (2001).

[239] Percentage derived from comparing comfort scores between scenarios within table 2 (78.3% - 41.2%).

[240] 18 U.S.C. § 2516(1)(a)-(u).

[241] *Id.* § 2518(3)(c).

[242] *Id.* § 2516(1).

[243] *Id.* § 2518(5) ("Every order and extension . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.").

[244] *Id.* § 2518(6) ("Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.").

Portions of this set of procedural protections would be appropriate in the facial recognition context as well. Focusing on more serious crimes also helps deal with concerns about pretextual uses.[245] A political protest might be in violation of a variety of incidental laws—unlawful assembly, obstruction of traffic, littering—and it would be problematic, both normatively and in the eyes of the respondents, for investigations into those offenses to serve as justifications for using facial recognition on a political gathering. In contrast, the kinds of investigations for which people were comfortable with facial recognition—homicide and auto theft—are not common accompaniments to peaceful political protests. For using facial recognition for mere identification, then, statutes should require 1) at least a warrant and 2) an investigation of a serious crime. Requiring such a burden mitigates the risk that a police officer is going to use facial recognition for pretextual investigations or their own personal benefit. This proposal is consistent with Professor Ferguson's recommendations: he also believes that a probable cause warrant and a restriction to serious crimes is appropriate here.[246] It also follows the broad guidelines of the Center proposal.[247]

The additional Wiretap Act requirements (that alternative means be exhausted, that only certain officials can request wiretap warrants, and minimization) are harder to assess. Fewer warrants would be issued given those requirements, but their imposition would not obviously tailor the frequency of warrants to the factor most relevant to the public, namely crime severity.

Moving beyond photo or video identification raises the question of face tracking over time and live person location. Public comfort levels here differ sharply from Professor Ferguson's and the Center on Privacy and Technology's prior proposals. The data suggest that respondents' comfort levels do not change greatly when facial recognition is used to locate, rather than identify, a worthy suspect or to track their historical location. Study 1 asked respondents for their comfort levels with (1) using facial recognition to identify a static image of a suspect in an auto theft case and (2) using facial recognition in a live search of an entire city for a suspect in an auto theft case. As noted above, the scenarios were described identically with the technique being used as the only difference. Although people were reliably more comfortable with the identification of the static image than with the live search, the difference was quite small: a difference of only 3.3%.[248] This difference is quite modest. When Study 3 further investigated this, considering the issue of tracking

---

[245] For a discussion of how purpose creep and pretext could create problems in the facial recognition space, see Ferguson, *supra* note 4, at 1162-63, 1205-07.

[246] *Id.* at 1199–1202; *see* Facial Recognition Act of 2022, H.R. 9061, 117th Cong (2022).

[247] Garvie, Bedoya & Frankle, *supra* note 31 at https://perma.cc/U2GY-JL5U.

[248] A within-subjects ANOVA was conducted comparing just those two scenarios. The test was significant $F(1, 957) = 14.06$, $p < .001$ $\eta^2 = .014$. The means are as reported in Tables 2 and 3. The 3.3 percentage point was arrived at by comparing the comfort scores in Tables 2 and 3 (71.8%-68.5%).

over time via archival footage, again the difference with identification was not large.

Professor Ferguson's preferred solution is to ban this kind of face tracking.[249] As a second-best substitute, he believes that a treatment on par with the full Wiretap Act requirements is appropriate.[250] Fundamentally, he thinks it is best that the system never be built. The Center's proposal is similarly reflective of deep concern.[251] Public attitudes do not go so far, however. People support the use of the system to locate suspects in serious crimes, and other people in a variety of emergency situations. Channeling public attitudes would not support a ban on face tracking. People do not view it as so fundamentally different from mere identification.

On this point it may be particularly important to consider democratic values. The specter of a government readily searching all the cameras in a city for a suspect is especially dystopian. Even if mere identification does not require the full process of a Wiretap Act-style super warrant, live tracking should. The state should have to show that other reasonable means have been exhausted or are impractical and have the sign-off of a more senior official. That would prevent live tracking from becoming an everyday tool while preserving it as an option for more serious offenses.

Finally, a statute based on public attitude should include an emergency carve-out. Over 80% of respondents were comfortable using facial recognition to scan live video feeds to locate a missing child. States have already set up systems to notify broad sections of the public about lost children, potentially incapacitated seniors, and other missing people - the AMBER and SILVER alerts.[252] Using facial recognition here would simply be an extension of those existing programs. Further, an active shooter or national disaster situation might also justify the suspension of the normal procedural protections. This suspension of protections, however, can neither be total nor permanent and both ex ante documentation and retrospective auditing must be required.

V. CONCLUSION

Facial recognition has already been deployed, in a dozen ways, by various government agencies. The technology is here. This Article aims to walk the line between the status quo of unfettered facial recognition and prospect of a

---

[249] Ferguson, *supra* note 4, at 1202–05.

[250] *Id.*

[251] Garvie, Bedoya & Frankle, *supra* note 31 at https://perma.cc/U2GY-JL5U, recommendation 6.

[252] Dawn Carr et al., *Silver Alerts and the Problem of Missing Adults with Dementia*, 50 GERONTOLOGIST, no. 2, 149 (2010), https://perma.cc/5TYK-6VKM; *Silver Alerts Notify the Public When an At-Risk or Vulnerable Senior Goes Missing*, WIS. CRIME ALERT NETWORK, https://perma.cc/KJ3Y-EUWV .

government artificially hobbled by blanket prohibitions on its use. Its proposal recognizes the comfort many Americans feel with targeted use of facial recognition, and its prospective utility in tasks both commonplace and fantastical. But it also recognizes that Americans reject universal face surveillance. The only way to respect that rejection is by granting some privacy in otherwise public spaces. To grant, by statute if not by constitutional provision, the right to walk down the street without being automatically identified at the whim of a state actor.

1. APPENDIX A: DEMOGRAPHICS OF THE SAMPLES

The sample for Study 1 was recruited by Dynata. The sample from Study 2 came from CloudResearch.

Table A1: Demographic Data for Each Survey

	Study 1	**Study 2**		**Census**[253]
Gender				
Female	50.4%	52.7%	50.3%	50.8%
Male	49.2%	46.8%	49.2%	49.2%
Other	0.4%	0.5%	0.5%	
Age (Years)[254]				
Median	48	44	46	
Mean	48.52 (17.68)	44.89 (16.12)	47.14 (17.00)	
Political Orientation (1–7)[255]	3.98 (1.82)	4.12 (1.79)	3.05 (1.18)	
Race and Ethnicity				
White	77.2%	72.7%	77.4%	76.3%
Black or African American	13.5%	20.8%	16.8%	13.4%
American Indian or Native American	0.6%	1.3%	1.1%	1.3%
Asian American	5.0%	2.0%	1.2%	5.9%
Hawaiian or Pacific Islander	1.1%	-	.2%	0.2%
Multiracial or Other	2.5%	3.2%	3.2%	2.8%
Hispanic (of Any Race)	18.2%	10.2%	7.2%	18.5%
Educational Attainment				
Less Than High School Diploma	9.1%	3.9%	3.0%	10.9%
High School Diploma or GED	27.7%	31.1%	25.9%	28.6%
Two-Year or Some College	25.6%	37.7%	34.4%	28.2%
Four-Year College	23.0%	16.4%	24.1%	20.6%
Graduate Degree	14.7%	10.9%	12.6%	11.6%

[253] Ethnicity and gender statistics are from the U.S. Census website. *See QuickFacts*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts//fact//table//US//PST045217 [https://perma.cc/S5BR-9P3J] (last visited Jan. 31, 2023). Educational attainment was calculated from data in table 1 in *Educational Attainment in the United States: 2018*, U.S. CENSUS BUREAU (Apr. 17, 2020), https://www.census.gov/data/tables/2018/demo/education-attainment/cps-detailed-tables.html [https://perma.cc/Q458-PS5U].

[254] A few participants entered what appeared to be their year of birth rather than their age. In those cases, data were recoded to reflect what their age would have been were that the case.

[255] Political orientation was assessed on a scale ranging from 1, very liberal, to 7, very conservative.

2. APPENDIX B: FULL TEXT OF SCENARIOS FROM STUDY 1

Overall description and instructions:

The questions in this survey concern facial recognition technology. Generally speaking, facial recognition technology enables a computer to compare a person's face against either a single image ("Is this Bob?") or a group of images ("Is this one of the students in the class? Which?") to see if it can find a match.

The questions on the next few pages will ask you to consider how you feel about different governmental uses of facial recognition. Please read each question carefully.

General Uses

1. A city government puts facial recognition equipped cameras opposite the entrances to private venues that host Alcoholics Anonymous meetings. These are often held in churches and community centers. People entering near meeting times are identified by comparing their faces to the state driver's license database.
2. A city's mayor uses facial recognition equipped cameras to identify people attending the campaign rallies held by their opponent in an upcoming election. The rally attendees are identified by comparing their faces to the state's driver's license database.
3. A city's government puts facial recognition equipped cameras in a public park around the time of a free show sponsored by the Parks Department. People attending the show are identified by comparing their faces to the state driver's license database. The department later sends them flyers about future shows and invitations to donate to support the arts.
4. A public hospital uses facial recognition to check in returning patients. Patients entering the waiting room are scanned and their faces are matched against an array of patients expected that day. People who do not match check in at a desk.
5. As people enter a public high school, their faces are compared to the list of approved people (students, faculty, staff) by a facial recognition camera mounted at each entrance. People who do not match are stopped by a security guard.
6. As people returning to the US from another country pass through customs, they present their passport to a computer that uses facial recognition to compare their face to the image on the document.
7. A public hospital uses facial recognition to identify an unconscious person who was brought in by ambulance and did not have identification on them. The program tries to match the person's face with an image from the state driver's license database.

Law Enforcement Use

1. Traffic enforcement authorities use facial recognition equipped cameras to identify jaywalkers by comparing their faces to the state driver's license database. Suspected jaywalkers are then mailed tickets.
2. A homicide detective uses facial recognition to identify someone who appears to have witnessed a murder outside a bodega. The bodega's security camera shows the man was standing across the street at the time of the crime. The software compares the image of the witness to the state's driver's license database.
3. A detective uses facial recognition technology to identify a person suspected of stealing a car that had been parked overnight outside a bodega. The software compares the image from a bodega security camera to the state's driver's license database.
4. A homicide detective uses facial recognition technology to identify a person suspected of killing a man outside a bodega. The software compares the image from a bodega security camera to the state's driver's license database.

Live Monitoring

1. A local police force uses street cameras to scan the faces of people in the crowd at a city marathon in real time. The marathon observers' faces are compared to a list of people with outstanding warrants. If a match is found, police are notified.
2. A detective uses facial recognition technology to scan all public cameras in a city to locate a person suspected of stealing a car that had been parked overnight outside a bodega. The software compares the image from a bodega security camera to a live feed of all city owned cameras, including those on public buses, in public parks, and on street corners. When a match is found, the detective is notified of the suspect's real-time location.
3. The Transportation Security Agency uses an airport's security cameras to scan the faces of people who enter the airport in real time. Their faces are compared to a list of people who are on no-fly lists or suspected of being terrorist threats. If a match is found, security is notified.
4. A detective uses facial recognition technology to scan all public cameras in a city to locate a missing child. The software compares the image provided by the child's parents to a live feed of all city owned cameras, including those on public buses, in public parks, and on street corners. When a match is found, the detective is notified of the child's real-time location.