THE CENTURY FOUNDATION | 1919 2019

REPORT SURVEILLANCE & PRIVACY

Preserving the Right to Obscurity in the Age of Facial Recognition

OCTOBER 20, 2017 — JAKE LAPERRUQUE

> *“Police suggest entire population in the Elm Terrace area do as follows: Everyone in every house in every street open a front or rear door or look from the windows. The fugitive cannot escape if everyone in the next minute looks from his house. Ready!”*
>
> *“Of course! Why hadn’t they done it before! Why, in all the years, hadn’t this game been tried! Everyone up, everyone out! He couldn’t be missed!”*[1]

Ray Bradbury’s vision of a future of pervasive surveillance in a*Fahrenheit 451* was perhaps not ambitious enough. Today, the government does not need to call on the populace to act with a million eyes to find a specific person, anywhere, at any time. With facial recognition technology, the government can do this, on its own, with the push of a button.

This technology not only exists: it is already in place, and in use, for surveillance efforts across the country. It operates via massive networks of cameras, together with extensive government databases of photographs tagged and compiled into profiles. Law enforcement use powerful computer algorithms to parse stockpiles of camera footage, picking out every face in a particular scene and rapidly associating them with profiles in the databases.

The ubiquity of networked surveillance cameras makes targeted facial recognition surveillance possible at essentially any place and any time. Law enforcement has more and more cameras every day, including CCTV cameras, police body cameras, and even cameras on drones and surveillance planes hovering over cities, which have already been used to record mass protests.[2] The FBI’s Next Generation Biometric Identification Database and its facial recognition unit, FACE Services, can already search for and identify nearly 64 million Americans, from its own databases or via its access to state DMV databases of photo IDs.

With the records already in hand, the technology in place, and the system’s capabilities rapidly growing, it may be soon that government will be able to find out who you are, where you’ve been and when, and who you’ve associated with simply by putting your name into a search bar.

With the records already in hand, the technology in place, and the system’s capabilities rapidly growing, it may be soon that government will be able to find out who you are, where you’ve been and when, and who you’ve associated with simply by putting your name into a search bar. In this way, facial recognition heralds the end of obscurity.

Despite this imminent danger, hardly any limits have been placed on this use of facial recognition technology. It was not until March of this year that Congress held a hearing to discuss the risks of facial recognition surveillance, and no laws—state or federal—exist that impose restrictions on how facial recognition surveillance can be used, and who it can target. Because of this absence, facial recognition can be used to circumvent existing legal protections against location tracking, opening the door to unprecedented government logging of personal associations and intimate details of citizens' lives.

Facial recognition could also become a dangerous tool for cataloging participation in First Amendment activities. Religious and political associations could become known to the government on an enormous scale, with little effort or cost, enabling disruption, persecution, and abuse. American history throughout the twentieth century and recent government activities in the past two decades both demonstrate that fear of such abuse is quite warranted.

As with any powerful tool, however, facial recognition also holds promise of being extraordinarily helpful—such as in finding missing persons, or identifying dangerous fugitives at large—and could provide significant public benefits without controversy. So, as alarming as facial recognition surveillance may be, policy that limits its use can provide a reasonable middle ground, one that prevents abuse and addresses the risk it poses of chilling First Amendment activities, while also permitting use for legitimate, and broadly supported, public safety purposes.

This report lays the groundwork for these policy efforts by offering explication of the technology's existing and potential uses, and the most concerning aspects of the threats its use poses to democracy. It follows with an overview of the essential aspects of an effective policy response, including whether facial recognition surveillance should require judicial authorization at a probable-cause standard for scanning a specific face in a photo or video to identify that individual, and whether limits should be enacted on the crimes for which facial recognition surveillance can be used as a response. And, because implementation of such a policy response within a necessary timeframe may prove difficult at the federal level, the report presents a "reverse-federalism" approach to advocacy and legislation, in which the FBI's dependence on state DMV photo databases is leveraged to promote state laws that, from below, impose effective policy limits on facial recognition surveillance at the national level.

Left unchecked, facial recognition will soon bring an end to obscurity. Obscurity may not seem like a fundamentally important value. It was not lauded in the Federalist Papers, inscribed in the Constitution, or mentioned as part of the "Four Freedoms" we fought to preserve in World War II. And yet, poetically standing unnoticed in the background, obscurity has served as a critical pillar to American democracy. Democracy by its nature relies on anonymity of some activities and interactions, especially in First Amendment activities like protests and religious worship. For over 200 years, obscurity has been one of anonymity's most powerful defenses. These protections are in grave danger, and their survival requires a swift and innovative policy response.

The Growing Power and Use of Facial Recognition

Despite the relatively low level of focus it has received in public debate, facial recognition is already a powerful and broadly used government surveillance tool, with its capabilities and deployment likely to continue to expand in the future. Current face-scanning technology is powerful, permitting rapid identification, and the potential is growing for real-time scans of entire crowds to identify individuals. Law enforcement already employs facial recognition on a huge scale, with the ability to track the activities of hundreds of millions of Americans. And technological advances in a range of areas regarding video technology will dramatically enhance the power of facial recognition, as the government becomes more able to record extensive public spaces, using facial recognition technology to identify any and every person caught in these nets of video surveillance.

Facial Recognition Technology

Facial recognition technology provides immense identification power, far beyond anything possible by human eye alone, even by entire police departments. Generally, facial recognition technology consists of software that allows computers to do what, until recently, was only capable by the human mind: recognize and identify faces. It uses facial features—such as the location of eyes in relation to the face as a whole—to create a "face print" that, like other forms of biometric identification, is unique to each individual. Facial recognition technology can then run an image of a face against an existing database of face prints and, if a match occurs, identify the individual.

EXAMPLE OF FACIAL RECOGNITION TECHNOLOGY UTILIZING A NODAL MAP.

Currently, facial recognition technology can scan for a match to identify a face againsttens of millions of pre-identified face profiles per second.[3] And real-time facial recognition surveillance is rapidly developing. A March 2017National Institute of Standards and Technology report concluded that while still difficult, real-time facial recognition is achievable with certain algorithms.[4] And practically all major private facial recognition companies already highlight their real-time facial recognition capabilities.[5]

Law Enforcement Use of Facial Recognition Surveillance

Law enforcement is already deploying facial recognition technology on a broad scale. According to a report by the Georgetown Law Center on Privacy and Technology, one in two American adults are already have their images stored in a law enforcement facial recognition network,[6] and at least one in four police departments have the capacity to run facial recognition searches.[7] In some cities, local law enforcement uses facial recognition for routine traffic stops, with little transparency as to its retention and subsequent use of acquired data.[8] The Department of Homeland Security (the DHS) is considering deploying facial recognition as a major component of its international travel security efforts,[9] as well as deploying drones equipped with facial recognition capabilities along the border.[10] And legislation in Congress could rapidly expand these surveillance behaviors, requiring the DHS to create a facial recognition database of immigrants, use facial recognition technology at airports, and create a biometric exit system at the fifteen largest airports, seaports, and land ports in the country.[11]

However, the largest and most worrisome facial recognition program already underway is the FBI's Next Generation Biometric Identification Database and its facial recognition unit, FACE Services. Nearly 64 million Americans are already subject to FACE Services' facial recognition searches from the FBI's database—composed of mug shots and photos of government employees—or via its access to state DMV databases, which serves as a backbone for the database.[12] According to a Government Accountability Officestudy, the FBI's FACE Services runs an average of 4,055 facial recognition searches per month through this system.[13]

Especially concerning has been law enforcement's development of real-time facial recognition surveillance, which it performs through the use of networks of both publicly and privately installed video cameras. Major cities including Chicago, Dallas, and Los Angeles are all engaged in, or considering development of, real-time facial recognition;[14] and during a March 2017 hearing on facial recognition surveillance, the FBI would neither confirm nor deny if it uses real-time facial recognition surveillance.[15] The CEO of Axon, America's largest police body camera seller, states, "There's a ton of interest in getting better real-time information . . . real-time analytics are going to be very interesting."[16] According to a Justice Department-funded study, nine of thirty-eight body camera manufacturers have already incorporated facial recognition technology into their products, or have the capacity to do so in the future.[17]

With its capacity to scan large crowds and identify anyone at any time, and all at very little cost, it is no surprise that the Georgetown Center on Privacy and Technology states, “Real-time face recognition marks a radical change in American policing—and American conceptions of freedom.

These investments mirror those made in the surveillance practices of autocratic states such as Russia, in which real-time facial recognition is already being deployed for troubling purposes.[18] With its capacity to scan large crowds and identify anyone at any time, and all at very little cost, it is no surprise that the Georgetown Center on Privacy and Technology states, “Real-time face recognition marks a radical change in American policing—and American conceptions of freedom. . . . There is no current analog—in technology or in biometrics—for the kind of surveillance that pervasive, video-based face recognition can provide.”[19]

The Increasingly Pervasive Nature of Law Enforcement Video Surveillance

The most worrisome aspect of the advance in facial recognition surveillance is not improvements in the technology itself—already astoundingly powerful—but rather the rapid expansion, both in capabilities and use, of video recording technology. Its expansion provides the government with an ever-broadening panopticon, wherein, because ever more faces are being captured on camera, ever more people are being tracked using facial recognition.

Video surveillance technology is enhancing the scope of government’s facial recognition surveillance in a variety of ways. First, the use of CCTV and police “blue light” cameras—CCTV cameras owned and operated by police departments for public safety—is expanding in many cities.[20] Second, advances in aerial technology offers new means of video surveillance. Drones and high-altitude piloted planes, such as those employed by Baltimore’s Persistent Surveillance programs, offer law enforcement the ability to rapidly zoom in on any specific area of a city down to a level where face scans can be run.[21] And new military camera technology such as the ARGUS-IS could soon allow government to continuously record areas up to ten square miles—roughly the size of half of Manhattan—and with the precision to scan the face of anyone and everyone in that entire citywide field, at any time.[22]

Perhaps the most daunting implications of growing facial recognition capabilities due to advances in video surveillance technology come from police body cameras. While not yet on every officer, most of America’s largest cities, if they don’t already require body cameras, are now deploying them in pilots and trials, with the expectation of moving toward universal use.[23] This would effectively turn every police officer into a camera capable of facial recognition scanning, expanding the scope of police video surveillance beyond even those departments with the most aggressive CCTV camera systems.[24] For example, police cameras in Chicago—which employs one of the nation's largest "blue light" camera systems—would have law enforcement cameras increase five-fold if all its officers wore body-cameras.[25] Yet the vast majority of cities and departments place no limits on use of facial recognition in conjunction with body cameras,[26] with only Oregon prohibiting their combined use.[27] And as mentioned above, the market is fast closing in on these developments in police practice: Axon, America's largest body camera vendor, has committed to adding facial recognition technology to all of its devices in the near future,[28] while also offering its cameras free for year-long trial periods to encourage their use.[29]

It is clear that technological limits will not stop facial recognition and accompanying tools from soon achieving the power to identify virtually anyone at any time. As the next section will explain, this would have immense ramifications on privacy rights and civil liberties, and fundamentally endanger democratic society.

How Facial Recognition Endangers Privacy Rights and Civil Liberties in a Manner Incompatible with Democratic Society

Facial recognition surveillance, absent proper checks and limits, is one of the most serious threats to privacy and civil liberties for a variety of reasons.

First, as executive director of the Georgetown Center on Privacy and Technology Alvaro Bedoya highlights, facial recognition surveillance is unique as an identification system in that, at present, its use does not require consent, or even notification.[30] Even if delayed for investigative purposes, notification is often a critical component of regulating invasive surveillance,[31] as it affords affected individuals the means to seek recourse against improper or overbroad actions. But individuals subject to facial recognition surveillance have little means of objection or recourse, and government has few checks on its actions. Additionally, an operational facial recognition system is largely unconstrained in terms of scale: government programs can enlarge the scope of its facial recognition capabilities from dozens to thousands of people with little increase in resources. Although its scale is already immense, the current FBI FACE Services average of 4,055 facial recognition searches per month might actually be quite low when compared to the system's capabilities and potential use in the future.

These factors make facial recognition surveillance especially worrisome as regards two of its uses: location tracking and the cataloging of First Amendment activities.

Location Tracking

While facial recognition is currently used most frequently for identification at a set time and location for investigative purposes,[32] technology and the growing presence of cameras has already enabled government to use facial recognition for location tracking. Even if such tracking would hardly ever be continuous, pinging an individual's location whenever they walk in range of cameras scattered throughout a city—or a powerful camera hovering in the sky—could effectively allow government to map out individuals' movements for weeks at a time.

This would severely undercut privacy rights, especially regarding location privacy. The Supreme Court has ruled that location tracking via the attachment of GPS devices requires a probable-cause warrant,[33] and will soon take up a highly important case to assess whether location tracking via cell phones should similarly require a warrant.[34] Even if the Supreme Court does not extend a constitutionally based warrant protection for cell-site location tracking, federal statute requires that the government go before a court and provide specific and articulable facts that such tracking is relevant to an ongoing investigation,[35] a rule that limits the scale of requests that can be made even though the standard of demonstrating relevance to an investigation is fairly easy to achieve. Furthermore, ten states have already enacted laws requiring a warrant for cell-site location tracking.[36]

But facial recognition-based location tracking could circumvent these protections, allowing the government to track individuals absent any suspicion of wrongdoing. Requiring that this type of surveillance receive prior judicial approval would not only ensure tracking is connected to criminal investigations: it would also limit its scale. Absent such requirements, location tracking could be practiced on a massive scale, continuously monitoring huge numbers of people in an automated manner. The only limits would be input decisions, the range of the cameras used, and data storage capacity.

Given its current potential, location tracking could have seismic effects on democratic society. Justice Sotomayor warned the nation thus in *United States v. Jones*:

> *[Location tracking] generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . [B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility. . . ." The net result is that GPS monitoring—*

> *by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society.*[37]

Because the costs of facial recognition surveillance, like those of GPS surveillance, are dependent on infrastructure rather than on number of targets, the only manner in which Justice Sotomayor's statement does not ring equally true for both forms of tracking is that it *underestimates* how low the cost—and thereby how great the risk of abuse—facial recognition-driven location tracking truly has.[38] If location tracking via GPS is too significant a risk to democracy to permit without court approval, then certainly so is tracking via facial recognition surveillance.

Cataloging First Amendment Activities

The most concerning risk that facial recognition surveillance poses is how it could impact First Amendment-protected activities. Absent proper restrictions—principally in the form of judicial authorization based on an appropriate level of suspicion—facial recognition could become an unprecedented tool for cataloging participation in a variety of First Amendment activities, and, subsequently, dramatically increase government's powers to target for persecution.

For example, government could take a photo or video of a large protest or political rally and use facial recognition to identify every participant. In a demonstration on facial recognition, the FBI in fact used political rallies as an example where the technology could be applied.[39] Similarly, cameras could easily be placed outside a church, synagogue, or mosque, and facial recognition used to identify every person who enters or exits.

Even without immediate identification, there is also a risk that government could build databases of metadata profiles of participants in these activities for further use. For example, rather than attempt to run face matches and identify participants, government could simply develop face prints based on participation, such as "Baltimore Black Lives Matter Protester #347" or "Manhattan Mosque Attendee #455." These profiles could be developed based on repeat attendance at "events of interest," creating layered portraits of individuals' behavior over time. The profiles could then be used for selective action against activists or religious minorities.[40]

Fear of such abuse is quite reasonable given the history of surveillance directed at minorities and activists throughout U.S. history. As research demonstrates, the twentieth century was plagued with instances of political surveillance, so much so that abuse of government surveillance power seems to become a recurring pattern rather than an exception unless effective checks are put in place.[41] Surveillance targeted at minorities has been just as pervasive.[42] Most infamous among a long list of improper surveillance activities is the COINTELPRO program. As revealed by the Church Committee, for years the FBI, under the J. Edgar Hoover, engaged in unjustified and often illegal surveillance, and used the fruits of that surveillance for persecution:

> *Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. . . . Unsavory and vicious tactics have been employed—including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in deaths. Intelligence agencies have served the political and personal objectives of presidents and other high officials. . . . Sometimes the harm was readily apparent—destruction of marriages, loss of friends or jobs. . . . But the most basic harm was to the values of privacy and freedom which our Constitution seeks to protect and which intelligence activity infringed on a broad scale.*[43]

The abuses of COINTELPRO may be decades old, but they demonstrate a risk that is ever-present: surveillance provides the means for a wide range of targeted abuse, including enabling the use of sensitive information to disrupt, and even destroy, individuals' private lives.

And of course, surveillance of minorities and activists is not a thing of the past. For years the New York Police Department ran a surveillance unit tasked with targeting and monitoring the city's Muslim communities, an effort that was both a gross violation of civil liberties and highly ineffective.[44] In recent years, the Department of Homeland Security has conducted extensive surveillance of Black Lives Matter activists,[45] while the FBI conducted aerial surveillance for overbroad monitoring of all individuals engaged in protests in Baltimore in response to Freddy Gray's death while in police custody.[46]

Facial recognition makes this pattern of improperly targeted surveillance especially frightening because it for the first time would allow government to accomplish total identification of minorities and activists, at very little cost. And unlike a phone number or license plate, one's face is a form of identification that can never be changed or cast aside. For COINTELPRO, developing lists of "agitators" required extensive undercover work and the allocation of agents. Cataloging individuals and cross-checking repeat activities and associations were constrained by data storage and the need for manual analysis.[47] Even more contemporary political surveillance, such as the NYPD Muslim Surveillance Unit's activities—supported by computers for data storage and analysis—was met with many of these same constraints. For example, while in operation, the Muslim Surveillance Unit relied on individual labor, such as "Plainclothes detectives [that] mapped and photographed mosques and listed the ethnic makeup of those who prayed there," as well as informants informally known as "mosque crawlers" that provided descriptions of individuals[48] and "collected the names, phone numbers and addresses" of Muslims.[49] Individual analysts "trawled college websites and email groups to keep tabs on Muslim scholars and who attended their lectures."[50]

In contrast, political surveillance with facial recognition has virtually none of these limits. Setting up cameras, deploying a small number of personnel to take video, or simply relying on already present officers with body cameras conducting routine duties costs government very little, and provides it with the means to identify virtually every individual at a protest, political rally, or religious ceremony, automatically and nearly instantaneously. Using those scans, metadata profiles can be created, cross-checked against other activities, and turned into extensive data profiles with little manual effort: How often does a certain individual go to their mosque? In which cities has an immigration rights activist protested? How many rallies has a Bernie Sanders supporter attended? For COINTELPRO, answering these questions for a single person might have required significant resources, but for today's government using facial recognition, it could merely require the click of a button to catalog corresponding data for thousands of people.

There is no federal statute limiting the use of facial recognition in any way, meaning no legal restriction exists to prevent these types of abuses. The FBI currently does not require any reasonable suspicion of wrongdoing to conduct facial recognition scans; mere "allegation or information" indicating any criminal activity is sufficient.[51] And because these are internal agency rules rather than externally imposed legislative limits, they are subject to unilateral change at any time, without public input or approval. As Chief Justice Roberts eloquently said in the landmark *Riley v. California* decision, which extended privacy rights on the basis of technological advance, self-imposed administrative limits are "probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols."[52]

Today, one does not need to be forced to register as a Communist to worry that they are on the government's watch and at risk of abuse: now anyone going to a protest, rally, or religious event is justified in fearing that they are being cataloged from afar, without their knowledge or any legal recourse to objection or response.

Even without such actions occurring, the mere possibility poses a threat that could cause major harm to First Amendment activities by making people frightened of exercising their right to them, thereby chilling participation. This chilling effect has already occurred with recent surveillance efforts directed at minorities. Studies show that in the wake of the NYPD's Muslim Surveillance Unit, many Americans were afraid to go to mosques or attend religious ceremonies.[53] And as previously discussed, facial recognition is a unique identification technique in that it requires neither consent nor notification. This amplifies the technology's potential to chill speech and religious activities whose participants worry they may risk persecution. Today, one does not need to be forced to register as a Communist to worry that they are on the government's watch and at risk of abuse: now anyone going to a protest, rally, or religious event is justified in fearing that they are being cataloged from afar, without their knowledge or any legal recourse to objection or response.[54] As then-House Oversight Committee Chair Jason Chaffetz stated during a March 2017 hearing on facial recognition surveillance, "It can be used in a way that chills free speech and free association by targeting people attending certain political meetings, protests, churches, or other types of places in the public."[55]

The new administration has done nothing to assuage these concerns. During the 2016 campaign, then-candidate Donald Trump called repeatedly[56] for the surveillance of mosques,[57] and even called for the creation of a national database of all Muslims in the United States,[58] and since becoming president has never renounced these alarming demands. After the election, former House Homeland Security Committee Chair Peter King explicitly invoked the NYPD Muslim Surveillance Unit as a model for the nationwide surveillance of Muslims.[59] Furthermore, during the campaign, Trump pledged to direct the attorney general to investigate Black Lives Matter activists, accusing the group of involvement in the murder of police officers.[60] During his confirmation, Attorney General Jeff Sessions refused to reject the possibility of using advanced surveillance technologies "to target and catalog individuals' exercise of First Amendment activities, such as religious activities, protests, and political rallies."[61] And during his confirmation, FBI Director Christopher Wray similarly refused to reject potentially conducting "general surveillance of mosques unrelated to a specific, ongoing investigation, or to conduct assessments or investigations of Muslim-American civil society leaders."[62]

Finally, absent limits on which crimes facial recognition could be used to investigate, facial recognition surveillance could become a means for "arrest-at-will" authority. Many municipalities have a huge number of active arrest warrants for minor crimes. For example, according to a 2015 Department of Justice investigation, Ferguson, Missouri had active arrest warrants—mostly for traffic violations, unpaid fines, and other minor offenses—for 16,000 people in a municipality with a population of 21,000.[63] This could give officers arrest-at-will authority, whereby an officer could conduct unannounced facial recognition scans during routine interactions with citizens, and whenever the officer is notified of an active bench warrant, they would then have the power to arrest the individual in question. This would create an unacceptable risk of selective action against minorities, protesters, or any other individual with whom officers choose to stop and engage. Additionally, if applied to all offenses, facial recognition surveillance could allow police to selectively scan large crowds—including protests and political rallies—and engage in mass arrests as a means of disrupting those events.

Given the potential for mass arrests or arrest-at-will authority, lawmakers should limit the set of crimes for which any form of law enforcement facial recognition can be used. These limits would perhaps become unnecessary if we were to adequately address the larger issue of over-criminalization, but given how unlikely such a response would be in the current administration, limiting use of facial recognition to certain crimes may be necessary to protect civil rights and civil liberties. Our government does not allow its most powerful and invasive surveillance tools to be used for minor crimes, so such a measure would not be unprecedented: the Wiretap Act proscribes a limited set of crimes for which audio surveillance technology may be used, and many complaints have been logged for the use of stingray location tracking[64] for the investigation of nonviolent crimes.[65]

In light of these risks, immediate action to place independent checks on facial recognition surveillance is not only necessary to prevent abuse, it is essential to stop the chilling of First Amendment activities that may already be occurring because of it.

How to Effectively Limit Facial Recognition Surveillance

Facial recognition surveillance, used judiciously, has the potential to provide unique public benefits, and should by no means be banned outright. Rather, policy should seek to place limits to reduce the potential for harm and abuse—that, even in the absence of misuse could still chill First Amendment protected activities—while still permitting selective use for public good. Precedents set for similar surveillance practices, such as wiretapping and the searching of smartphones, should be consulted in determining the threshold of permissibility for facial recognition surveillance and tracking.

Necessary Policy Limits on Facial Recognition Surveillance

The vast majority of potential abuses of facial recognition stem from use disassociated from independent authorization and proper level of suspicion. Requiring judicial approval at an appropriate standard would ensure that facial recognition could serve as an effective tool for law enforcement, but not lead to pervasive location tracking or improper targeting and persecution.

Therefore, facial recognition surveillance should require judicial authorization. This is critical as regards two of the technology's uses: first, scanning a specific face in a photo or video to identify that individual; and second, developing a metadata profile of a specific face at a given location, for the purposes of tracking that face's appearances in the future.[66] These situations should require particularization, meaning requiring that law enforcement obtain court approval for each individual person that facial recognition is to be applied to; mass face identification scans would not permitted.

The appropriate standard for such judicial authorization is probable cause, as this would put use of facial recognition on par with location tracking standards that already exist for GPS device tracking and cell-site tracking in many states. A lower standard would allow facial recognition surveillance to serve as a circumvention of these rules: for instance, if limited to reasonable suspicion, law enforcement could avoid warrant requirements for location tracking by using facial recognition for the same purposes instead. However, this probable-cause judicial authorization should also come with the same exceptions as similarly restricted measures: consent and emergencies should permit less-restricted law enforcement action. Additionally, facial recognition presents unique needs for other exceptions, notably for use in finding and identifying missing persons.

Additional limits beyond judicial authorization at a probable-cause standard should be enacted for the continuous scanning of cameras to locate or track individuals in real-time. This is necessary for several reasons. First, this type of facial recognition surveillance is not particularized: it involves scanning all individuals—absent suspicion—within a camera's range to determine if they match with a designated suspect. Second, rather than apply to a static moment in time, this type of surveillance would be continuous for a prolonged period of time. Third, while the practice of particularized identification involves a single location and camera—or at most a small set of cameras capturing the same location from multiple angles—continuous scanning could apply to extensive geographic areas and hundreds or even thousands of cameras.

In light of these concerns, it is necessary that government provide justification for the geographic scope and length of time of continuous facial recognition surveillance, and a general time limit should be required with judicial reauthorizations for extensions. Exhaustion requirements, which require law enforcement to first attempt less intrusive methods, or at least explain why they would be ineffective, should also be included. Finally, additional limits should be included to limit the scale of use for continuous facial recognition surveillance. A mix of former law enforcement and civil liberties experts recommend several potential means of achieving this: (1) Require top law enforcement officials—such as state attorneys general—to certify that such surveillance is necessary, (2) limit continuous scanning to situations where an active arrest warrant exists for a small set of violent crimes, (3) require connection to an ongoing threat of death or serious bodily harm, (4) limit continuous scanning to specific situations—such as large events or locations like stadiums—where there is heightened risk of harm to a large number of people, or (5) require a combination of these factors.[67] Each of these possibilities is worthy of additional debate and analysis.

Recommending a Novel Means of Efficiently Achieving Proper Limits on Facial Recognition Surveillance

While numerous advocates and organizations have advocated for some or all of the policy proposals described in the previous section,[68] I propose an entirely new means of achieving their implementation. The method I propose centers on the FBI's use of state DMV photos, without clear notice or approval of those submitting photos. This practice has rightfully been condemned as invasive, overbroad, legally tenuous, and excessively secretive: the FBI was rebuked during a House Oversight hearing on facial recognition surveillance this March for giving misleading testimony on whether it had access to state DMV photos.[69]

But I believe we can, and should, use the FBI's reliance on state DMV photos as a means to achieving broad reform of facial recognition surveillance. This dependence creates the opportunity to effectively target states for reform legislation, and, with a carrot-and-stick technique regarding access, push the FBI toward reasonable policies. With this "reverse federalism" approach, advocates can target the states that are most likely to enact privacy protections, and thereby potentially see those protections applied across the entire nation.

Why "Reverse Federalism" Is a Uniquely Effective Policy Approach for Facial Recognition

The most effective means of enacting these reasonable protections against overbroad facial recognition surveillance would be federal legislation, which would affect all law enforcement across the nation and be difficult to roll back. However, federal legislation in general faces a series of gatekeepers: committee chairs in the House or Senate, or overall leadership in either chamber, could single-handedly block a bill from moving forward, and it must achieve support of most members in committees, and the full House and Senate in order to pass. Surveillance reform legislation in particular has frequently failed to overcome these obstacles. Basic email privacy reform, for instance, has been mired in obstruction for nearly a decade despite widespread support.[70] Federal location privacy legislation, another example, has never even advanced to a committee vote, even as ten states have enacted warrant-for-location laws[71] and the Supreme Court is preparing to take on the issue.[72]

Facial recognition surveillance is highly unique in that the FBI—and any agency coordinating with them in reliance on their database—is highly dependent upon the cooperation of state-level agencies.

However, facial recognition surveillance is highly unique in that the FBI—and any agency coordinating with them in reliance on their database—is highly dependent upon the cooperation of state-level agencies, in that while the FBI has its own database of mugshot photos, a huge portion of the photos it uses for facial recognition searches come from accessing state DMV photo databases.[73]

This creates an opportunity for "reverse federalism," a situation in which state laws could influence federal policy. A carrot-and-stick approach could be applied by states across the country: states that do not provide DMV photos could offer to do so, on condition that the FBI enacts policies conforming to the rules set out above, offering an enticing opportunity to expand the scope and power of surveillance practices in exchange for reasonable limits on use. And states that already offer DMV photos for the FBI database could pass legislation stating that access will be revoked unless the FBI enacts policies conforming to these rules.

Agreements to access state DMV photos are not the only means by which the FBI gathers photos for facial recognition surveillance, but it is certainly the most significant. The FBI facial recognition system stores or can access "24.9 million mug shots, over 140 million visa photos and over 185 million state driver's license and ID photos."[74] However, the FBI is only able to access DMV photos via state agreements per the Driver Privacy Protection Act (DPPA), and even this process is legally questionable, as facial recognition surveillance was not envisioned when the DPPA was passed in 1994.[75] In 2016, law enforcement attempted to mine therich quantity of data on social media via the third-party app Geofeedia, but it quickly created a firestorm of demands that social media companies cut off access to the app, to which they acquiesced, demonstrating that these companies will not so willingly allow their services to be co-opted for facial recognition surveillance.[76]

This approach provides a variety of strategic benefits as regards more rapidly achieving proper limits for facial recognition surveillance. First, it provides more opportunities for action. Although state legislatures contain the same types of gatekeepers and pose the same types of obstacles as Congress does, multiplying the number of potential avenues of success in itself is an advantage. Second, states have always served as "laboratories of democracy." While the FBI may choose not to consent to the conditions set forward in legislation in a small number of states, if these policies are successful at the state level across the country, it would put added pressure on the FBI to adopt them as well. Most importantly, and as mentioned above, a reverse-federalism approach that allows advocates to work for reform at the state level will allow them to strategically choose the locations that are most politically favorable to achieving these goals. The next section will provide an analysis of what the best states for action might be, and the impact of legislation in these states in pressuring voluntary reform by the FBI.

Assessing Effective Points of Action

Effective advocacy to advance legislation and provide sufficient opportunities—and pressures—regarding state access to DMV photo databases will require efficient use of resources, targeting states where there is the best chance of success.[77] Based on prior legislative action on surveillance policy, the following describes two categories of states that are the best targets for enacting the legislation described above: first, and most promisingly, states that have already enacted, or are actively considering, legislation to restrict government use of facial recognition surveillance; and second second, states that have already enacted location privacy laws.

States already engaged in restricting facial recognition. States that have already enacted, or are actively considering, legislation to curtail facial recognition surveillance are the best areas to start reverse-federalism efforts, and thereby pressure the FBI to voluntary enact proper limits on its use of facial recognition. Legislatures in these states are already engaged with the issue, and so their members will be familiar with the acute risks facial recognition poses, and how sensible limits can protect privacy without unreasonably inhibiting law enforcement needs. There will be champions of the cause from these states' prior efforts to sponsor new legislation who lead these new efforts. If prior facial recognition legislation has advanced to votes, advocates will have a map of where to target efforts. And stakeholders—ranging from local law enforcement to civil rights advocates—will have experience in the issue, and will be adept in negotiating potential points of contention. For these reasons, the most promising states in which to begin advocacy are:

- **Maryland.** In 2017, legislation was introduced in the Maryland General Assembly to require a warrant for facial recognition surveillance.[78] However, the bill did not advance out of committee, demonstrating significant obstacles left to overcome before enacting facial recognition limits in the state. Maryland currently does not allow the FBI to use its DMV photo database, which includes face images of over 4.1 million people.

- **Oregon.** While it has not created a policy limiting facial recognition surveillance generally, in 2015 the state enacted a law fully prohibiting the use of facial recognition in conjunction with police body cameras.[79] Given that this was a full ban—not even permitting use of facial recognition with body cameras with judicial authorization based on probable cause—the passage of broader limits, with exceptions contingent on proper demonstration of cause, may be viewed as a reasonable compromise in the state. Oregon currently does not allow the FBI to use its DMV photo database, which includes face images of over 2.8 million people.

- **Rhode Island.** In 2017, as well as in previous years, legislation was introduced in the Rhode Island State Legislature to regulate drones, including a full prohibition of the use of facial recognition technology on any video footage captured by drones.[80] The bill has not received a vote in committee. Rhode Island currently does not allow the FBI to use its DMV photo database, which includes face images of over 745,000 people.

In total, if legislation were passed in these states, it would offer the FBI access to additional DMV photos from about 7.8 million people for its facial recognition searches. This could offer a strong incentive for the FBI to voluntarily change its policies on facial recognition.

States that have enacted warrant for location protections. States that have enacted laws requiring law enforcement to obtain a probable-cause warrant before tracking an individual's location may not have directly addressed facial recognition surveillance yet, but they are well-poised to appreciate its risks and respond to them. Legislatures in these states have recognized the sensitivity of personal location information, even (and sometimes especially) in public places, and therefore have already demonstrated some sympathy to the concerns that facial recognition surveillance poses. Additionally, because facial recognition can serve as a means of electronic location tracking, lawmakers may see legislation limiting its use as a means of preventing a loophole in the location tracking limits already enacted. Location privacy could serve as an effective proxy in focusing advocacy efforts, immediately suggesting which legislators may be receptive to limiting facial recognition surveillance based on their positions on earlier surveillance legislation. Finally, given experience with the power to conduct investigations—with prior judicial authorization—using location tracking, local law enforcement may be less resistant to the the imposition of similar limits on facial recognition tracking and identification. For these reasons, promising states for advocacy are:

- **California.** In 2015, California enacted a law requiring a warrant for historical and real-time location information.[81] California currently does not allow the FBI to use its DMV photo database, which includes face images of over 25.5 million people.

- **Illinois.** In 2014, Illinois enacted a law requiring a warrant for real-time location information,[82] including unanimous passage in the State Senate.[83] Illinois currently permits the FBI to use its DMV photo database for facial recognition searches, which includes face images of over 8.4 million people.

- **Indiana.** In 2014, Indiana enacted a law requiring a warrant for real-time location information, and also requiring a warrant for drone use.[84] This is notable in that drone surveillance offers government a means of location tracking without any recourse to third-party data or resources. Indiana currently does not allow the FBI to use its DMV photo database, which includes face images of over 4.4 million people.

- **Maine.** In 2013, Maine enacted a law requiring a warrant for historical and real-time location information.[85] Maine currently does not allow the FBI to use its DMV photo database, which includes face images of over 1 million people.

- **Minnesota.** In 2014, Minnesota enacted a law requiring a warrant for historical and real-time location information.[86] Minnesota currently does not allow the FBI to use its DMV photo database, which includes face images of over 3.3 million people, but in 2016, the Government Accountability Office reported the state was in negotiations to permit access.

- **Montana.** In 2013, Montana enacted a law requiring a warrant for historical and real-time location information.[87]

Montana currently does not allow the FBI to use its DMV photo database, which includes face images of over 781,000 people.

- **New Hampshire.** In 2015, New Hampshire enacted a law requiring a warrant for historical and real-time location information.[88] New Hampshire currently does not allow the FBI to use its DMV photo database, which includes face images of over 1 million people.

- **Utah.** In 2014, Utah enacted a law requiring a warrant for historical and real-time location information.[89] Utah currently permits the FBI to use its DMV photo database for facial recognition searches, which includes face images of over 1.9 million people.

- **Virginia.** In 2014 Virginia enacted a law requiring a warrant for real-time location information; this law was weakened the following year, but a law was enacted requiring a warrant for use of cell-site simulators.[90] Virginia currently does not allow the FBI to use its DMV photo database, which includes face images of over 5.8 million people.

- **Washington.** In 2015 Washington enacted a law requiring a warrant for use of cell-site simulators.[91] Washington currently does not allow the FBI to use its DMV photo database, which includes face images of over 5.5 million people.

In total, if legislation were passed in these states, it would have a huge impact on the FBI's Next Generation Biometric Identification Database. Such action would terminate FBI access to the DMV photos of over 10 million people. However, legislation would also provide the FBI with access DMV photos of over 47.5 million additional persons if the agency changed its facial recognition surveillance policies. Under such circumstances, the FBI would have enormous incentive to voluntarily adopt limits on facial recognition surveillance.

Beyond these states, there are several states where warrants for location tracking are required, but as a result of state court rulings rather than legislation: Florida, Massachusetts, and New Jersey. While court rulings do not provide the same benefits as do statutory protections—in that they do not tell us which lawmakers should be the focus of advocacy efforts—they do offer other opportunities. First, in these states, local law enforcement will be more accustomed to limits on location tracking, and therefore may be more prepared to accept limits on facial recognition tracking and identification. Second, court rulings may have beaten legislators to enacting these limits, but it is still possible that lawmakers would have otherwise been amenable to such privacy legislation. Finally, legislation limiting facial recognition surveillance could be introduced as a necessary means in providing clarity and preventing future litigation, given the potential for electronic location tracking using facial recognition technology.

While these states are not as appealing as targets for advocacy as those where warrants for location tracking are already required, as a result of legislative action, they may still be receptive to efforts to promote limits on facial recognition surveillance. Legislation in these states would, in Florida's case, remove over 14.2 million people's DMV photos from FBI access, which currently provides access to its DMV photo database; and, in the case of Massachusetts and New Jersey, would provide previously unavailable access to the DMV photos of over 11.2 million additional people.

Conclusion

With so many pivotal issues facing American society—policy matters that will shape millions of lives being debated and decided, democratic institutions that have served as pillars of our Republic being stretched to their limit, even basic social norms that have seemed integral to our nation being questioned—the right to obscurity may seem like an unworthy value on which to focus. But policy, institutions, and our most fundamental norms are dependent upon freedom of speech, association, and engagement. And at times of greatest risk, those activities rely not just on the First Amendment, but also upon obscurity. At darkest times, obscurity has been the tool to save minorities and activists from stigma, from persecution, and from government power run amok.

> At darkest times, obscurity has been the tool to save minorities and activists from stigma, from persecution, and from government power run amok.

Yet facial recognition has endangered the very concept of obscurity, and without swift action, it will soon become extinct. Limiting facial recognition to prevent surveillance abuses should not be controversial, and given the stakes, it should be far more of a priority than most lawmakers have thus far treated it. We cannot afford to wait: the time to act on this issue is now. And the best form of action is at the state level. Targeting those states most amenable to reasonable limits on facial recognition technology, and most receptive to advocacy, presents a unique opportunity to fast-track nationwide checks against improper facial recognition surveillance. If successful, such legislation will provide a necessary shield for democracy, and just in time, before we find our public lives without a shield at all.

Notes

1. Ray Bradbury, *Farenheit 451* (New York: Ballantine Books, 1953), 164.

[2] Ian Duncan, “FBI admits providing air support to Baltimore Police during Freddie Gray unrest,” *Baltimore Sun*, May 7, 2015, http://www.baltimoresun.com/news/maryland/crime/bal-fbi-admits-providing-air-support-to-baltimore-police-during-freddie-gray-unrest-20150506-story.html.

[3] Francis Bea, Digital Trends, “Goodbye, Anonymity: Latest Surveillance Tech Can Search Up to 36 Million Faces Per Second,” *Digital Trends*, March 25, 2012 https://www.digitaltrends.com/cool-tech/goodbye-anonymity-latest-surveillance-tech-can-search-up-to-36-million-faces-per-second/.

[4] Patrick Grother, George Quinn, and Mei Ngan, “Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects,” NISTIR 8173, *National Institute of Standards and Technology, US Department of Commerce*, March, 2017, http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf.

[5] Clare Garvie et al., “The Perpetual Line-Up,” *Georgetown Law Center on Privacy & Technology*, October 18, 2016, https://www.perpetuallineup.org/.

[6] This can involve law enforcement photo databases, other photo databases, such as DMV records, to which law enforcement maintains access, or a combination. See Ibid.

[7] Claire Garvie et al, “The Perpetual Lineup.”

[8] Timothy Williams, “Facial Recognition Software Moves From Overseas Wars to Local Police,” *New York Times*, August 12, 2015, https://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html?_r=0.

[9] Russell Brandom, “Facial recognition is coming to US airports, fast-tracked by Trump,” *The Verge*, April 18, 2017, https://www.theverge.com/2017/4/18/15332742/us-border-biometric-exit-facial-recognition-scanning-homeland-security; Frank Bajak and David Koenig, “Face scans for US citizens flying abroad stirs privacy issues,” *Associated Press*, July 12, 2017, https://apnews.com/acf6bab1f5ab4bc59284985a3babdca4.

[10] Jake Laperruque, “Questions to Ask as DHS Pursues Border Drones With Facial Recognition,” *Just Security*, April 27, 2017, https://www.justsecurity.org/40334/questions-dhs-proposes-border-drones-facial-recognition/.

[11] Cyrus Farivar, “Building America’s Trust Act would amp up privacy concerns at the border,” *Ars Technica*, August 15, 2017, https://arstechnica.com/tech-policy/2017/08/gop-senators-border-wish-list-drones-dna-collection-voice-scans-and-more/; Jenna McLaughlin and Kavitha Surana, “Immigration Bill Would Ramp Up Mass Surveillance at the Border,” *Foreign Policy*, August 10, 2017,http://foreignpolicy.com/2017/08/10/immigration-bill-would-ramp-up-mass-surveillance-at-the-border/.

[12] Claire Garvie et al, “The Perpetual Lineup.”; “Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,” GAO-16-267, *U.S. Government Accountability Office*, May, 2016, http://www.gao.gov/assets/680/677098.pdf.

[13] “Face Recognition Technology: FBI Should Better Ensure Privacy.”

[14] Claire Garvie et al, “The Perpetual Lineup.”

[15] United States. Cong. House. Committee on Oversight and Government Reform. “Committee to Review Law Enforcement’s Policies on Facial Recognition Technology. March 22, 2017,” U.S. Congress, House Committee on Oversight and Government Reform, 115th Congress, 1st session, Washington, D.C., https://oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology/.

[16] Alex Pasternack, “Police Body Cameras Will Do More Than Just Record You,”*Fast Company*, March 3, 2017, https://www.fastcompany.com/3061935/police-body-cameras-livestreaming-face-recognition-and-ai.

[17] Vivian Hung, Steven Babin, and Jacqueline Coberly, “A Market Survey on Body Worn Camera Technologies,”*John Hopkins University Applied Physics Laboratory*, November, 2016, https://www.ncjrs.gov/pdffiles1/nij/grants/250381.pdf; Ava Koffman, “Real-Time Facial Recognition Threatens to Turn Cops’ Body Cameras Into Surveillance Machines,” *The Intercept*, March 22, 2017, https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/.

[18] Daniil Turovsky, “The end of privacy: ‘Meduza’ takes a hard look at FindFace and the looming prospect of total surveillance,” *Meduza*, July 14, 2016,https://meduza.io/en/ feature/2016/07/14/the-end-of-privacy.

[19] Claire Garvie et al, “The Perpetual Lineup.”

[20] Ted Cox, “Number of Chicago Security Cameras ‘Frightening,’ ACLU Says,”*DNA Info*, May 9, 2013, https://www.dnainfo.com/chicago/20130509/chicago/rahm-boosts-number-of-security-cameras-frightening-number-aclu; Luke Broadwater and Justin George, “City expands surveillance system to include private cameras of residents, businesses,” *Baltimore Sun*, October 30, 2014,http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-citiwatch-20141029-story.html.

[21] Jake Laperruque, “Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance,” *Richmond Law Review* 51, symposium book, March 24, 2017,http://lawreview.richmond.edu/files/2017/03/Laperruque-513-website.pdf.

[22] Ibid.

[23] “Police Body Worn Cameras: A Policy Scorecard,” *The Leadership Conference and Upturn*, August, 2016, https://www.bwcscorecard.org.

[24] Jake Laperruque, “Ways to Use and Misuse Facial Recognition With Police Body Cameras,” presentation,*2016 Cato Surveillance Conferenc*e, December 14, 2016,https://cdn.cato.org/archive-2016/cc-12-14-16-06.mp4.

[25] Ibid.

[26] “Police Body Worn Cameras.”

[27] Oregon, H.B. 2571 (2015).

[28] Jake Laperruque, “Should Police Bodycams Come With Facial Recognition Software?”*Slate*, November 22, 2016, http://www.slate.com/articles/technology/future_tense/2016/11/should_police_bodycams_come_with_facial_recognition_softw

[29] Jake Laperruque, “Taser’s Free Body Cameras Are Good for Cops, Not the People,”*Wired*, April 15, 2017, https://www.wired.com/2017/04/tasers-free-body-cameras-good-cops-not-people/.

[30] “Committee to Review Law Enforcement’s Policies.” (“Face recognition lets law enforcement identify people from far away and in secret. It also lets them remotely identify large groups of people, not just the target of an investigation.”)

[31] See, e.g., The Wiretap Act.

[32] Claire Garvie et al, “The Perpetual Lineup.”

[33] *United States v.Jones*, 132 S.Ct. 945 (2012).

[34] *Carpenter v. United States*, OT 2017.

35. 18 U.S.C. 2703(d).

36. Peter Cihon, “Status of Location Privacy Legislation in the States,”*American Civil Liberties Union*, August 26, 2015, https://www.aclu.org/blog/free-future/status-location-privacy-legislation-states-2015.

37. *United States v. Jones,* 132 S.Ct. 945 (2012); Sotomayor, J., concurring; internal citations omitted

38. *The average cost of the GPS tracking of a single vehicle is estimated at $0.36 per hour. See Kevin Bankston and Ashkan Soltani, “Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones,” Yale Law Journal 123, January 9, 2014,http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones. But because multiple faces can be inputted for scans with virtually no additional resource requirements, the cost of location tracking via facial recognition surveillance is virtually zero once sufficient cameras and computing systems have been put into place.*

39. *Richard W. Vorder Bruegge,” Federal Bureau of Investigation, Facial Recognition and Identification Initiatives, slide 4, https://www.eff.org/files/filenode/vorder_bruegge-facial-recognition-and-identification-initiatives_0.pdf.*

40. *Any time an assessment is opened against an individual, they could be run against these metadata profile databases to see if a match occurs, and then, if so, subsequent action taken. Selective prosecution, enhanced searches and screenings, targeting for pressure to desist from certain activities, and targeting for recruitment as informants are just a few of the troubling actions that could follow.*

41. *“American Big Brother: A Century of Political Surveillance and Repression,”Cato Institute, https://www.cato.org/american-big-brother.*

42. *Alvaro Bedoya, “The Color of Surveillance,” Slate, January 18, 2016, http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_abo*

43. “Final report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate: together with additional, supplemental, and separate views, *U.S. Senate, Select Committee to Study Government Operations With Respect to Intelligence Activities (a.k.a. the Church Committee)*, April 26, 1976.

44. *“Factsheet: The NYPD Muslim Surveillance Program,”American Civil Liberties Union, https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program?redirect=factsheet-nypd-muslim-surveillance-program.*

45. *See, e.g., George Joseph, “Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson,”The Intercept, July 24, 2015, https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/.*

46. *Ian Duncan, “FBI admits providing air support.”*

47. *“Final Report of the Select Committee.”*

48. *“With cameras, informants, NYPD eyed mosques,” Associated Press, February 23, 2012,https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques.*

49. *Matt Apuzzo and Joseph Goldstein, “New York Drops Unit That Spied on Muslims,”New York Times, April 15, 2014, https://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html?_r=0.*

50. *Ibid.*

51. Federal Bureau of Investigation, “Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit,” Federal Bureau of Investigation, May 1, 2015,https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit ; “Committee to Review Law Enforcement’s Policies.”

52. Riley v. California, 573 U.S. ___ (2014)

53. Diala Shamas and Nermeen Arastu, “Mapping Muslims: NYPD Spying and its Impact on American Muslims,”Creating Law Enforcement Accountability & Responsibility Project, City University of New York School of Law, March 11, 2013, http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

54. In fact, last year police used a third-party service—Geofeedia—toidentify and catalog Black Lives Matter activists. The app has since been blocked from the major social media platforms from which it derived information for facial recognition identification, but law enforcement will soon not need private company aid to engage in this type of mass identification of protesters. Janko Roettgers, “Police Used Instagram, Facebook, Twitter to Monitor Black Lives Matter Protesters,” Variety, October 11, 2016, http://variety.com/2016/digital/news/instagram-twitter-faceook-geofeedia-aclu-1201885332/.

55. “Committee to Review Law Enforcement’s Policies.”

56. See, e.g., Jeremy Diamond, “Trump Doubles Down On Calls for Mosque Surveillance,”CNN, June 15, 2016, http://www.cnn.com/2016/06/15/politics/donald-trump-muslims-mosque-surveillance/.

57. Reena Flores, “Donald Trump: I Want Surveillance of Certain Mosques,”CBS News, November 21, 2015, http://www.cbsnews.com/news/donald-trump-i-want-surveillance-of- certain-mosques/.

58. Jeremy Diamond, “Trump Would ‘Certainly Implement’ National Database for U.S. Muslims,” CNN, November 20, 2015, http://www.cnn.com/2015/11/19/politics/donald-trump-barack-obama-threat-to-country/ .

59. Christopher Mathias, “Rep. Peter King Urges Donald Trump to Create a Federal Muslim Surveillance Program,” Huffington Post, December 15, 2016,http://www.huffingtonpost.com/entry/peter-king-muslim-surveillance-trump_us_5852fdcae4b0b3ddfd8bc377.

60. Reena Flores, “Donald Trump: Black Lives Matter Calls For Killing Police,”CBS News, July 19, 2016, http://www.cbsnews.com/news/donald-trump-black-lives-matter-calls-for-killing-police/.

61. “Nomination of Jeff Sessions to be Attorney General of the United States: Questions for the Record,” questions posed by Sen. Richard Blumenthal, 115th Congress, 2017, 19-20, https://www.judiciary.senate.gov/imo/media/doc/Sessions%20Responses%20to%20Blumenthal%20QFRs.pdf.

62. “Nomination of Christopher Wray to be FBI Director of the United States: Questions for the Record,” questions posed by Senator Mazie Hirono, 115th Congress, 2017, 53, https://www.judiciary.senate.gov/imo/media/doc/Wray%20Responses%20to%20QFRs.pdf.

63. “Investigation of the Ferguson Police Department,” United States Department of Justice, Civil Rights Division, March 4, 2015, 55, https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report_1.pdf.

64. This forms of location tracking involves the use of IMSI catchers, commonly called “stingrays,” which imitate cell phone towers in order to receive data from all cell phones in a given area. Using these devices, law enforcement can

obtain location data with extreme accuracy.

65. *e.g. Nicky Woolf, "Lawmakers demand details on federal use of Stingray phone surveillance," The Guardian, November 9, 2015, https://www.theguardian.com/us-news/2015/nov/09/congress-stingray-surveillance-jason-chaffetz-elijah-cummings/ .*

66. *It is important to note that these situations involve facial recognition technology for identification, not face matching technology. Face matching is a similar but distinct process whereby software compares the images of two faces and determines whether or not they are they same. While the technology employed to achieve this is similar to facial recognition, the process poses far less risks to privacy as it involves comparing just one set of pre-identified faces, rather than identifying anonymous individuals. While some level of standard of suspicion may be appropriate for various face-matching activities, it is important to distinguish face matching from facial recognition, as the latter is the sole focus for this paper, and only area where recommended policy rules will be provided.*

67. *Kami Chavis, James Trainum, and Jeffrey Vagle, "Law Enforcement Facial Recognition Is a Powerful Surveillance Technology In Need of Independent Checks and Limits," The Constitution Project, March, 2017, https://constitutionproject.org/wp-content/uploads/2017/03/Facial-Recognition-Statement-for-Record_The-Constitution-Project.pdf.*

68. *See e.g. Claire Garvie et al, "The Perpetual Lineup;" "Committee to Review Law Enforcement's Policies," statement of Jennifer Lynch, Senior Staff Attorney, The Electronic Frontier Foundation; Kami Chavis, James Trainum, and Jeffrey Vagle, "Law Enforcement Facial Recognition."*

69. *"Committee to Review Law Enforcement's Policies:"*

FBI DEPUTY ASSISTANT DIRECTOR, CRIMINAL JUSTICE INFORMATION SERVICE DIVISION, KIMBERLY DEL GRECO: The only information the FBI has, and has collected in our database, are criminal mugshot photos, we do not have any other photos in our repository—

HOUSE OVERSIGHT CHAIRMAN, JASON CHAFFETZ: That's not true. You're not collecting drivers' licenses?

DEL GRECO: We do not have drivers licenses photos in our repository at the FBI

CHAFFETZ: …Mr. Bedoya?

GEORGETOWN CENTER ON PRIVACY AND TECHNOLOGY DIRECTOR, ALVARO BEDOYA: I think this is a technicality. Who owns and operates a database matters a lot less than who uses it, and how it's used. The FBI has access to now eighteen states' driver's license photos and can either run those searches or request them. We're talking more than a third of all Americans. So the FBI does have access to these photos, searches them tens of thousands of times…

CHAFFETZ: Would you disagree with that, Ms Del Greco?

DEL GRECO: We have access to the data, we do not maintain the data in our repository…

HOUSE OVERSIGHT RANKING MEMBER, ELIJAH CUMMINGS: Ms. Del Greco, when the Chairman asked you about what photos you had, you said over and over again we just have mugshots… I just feel…if I was left with your answer, and didn't have clarification, I would have assumed that's it. But they were able to clarify, these other two witnesses, that you have access to all kinds of photos… I just think it's unfair to the Committee. I usually don't do this, but it left me feeling not very good. And I'm sure the Chairman felt the same way.

70. *Mike Orcutt, “Why Congress Can’t Seem to Fix This 30-Year-Old Law Governing Your Electronic Data,” MIT Technology Review, February 17, 2017, https://www.technologyreview.com/s/603636/why-congress-cant-seem-to-fix-this-30-year-old-law-governing-your-electronic-data/.*

71. *See endnote 33.*

72. *See endnote 31.*

73. *Claire Garvie et al, “The Perpetual Lineup.”*

74. *Claire Garvie et al, “The Perpetual Lineup.”*

75. *“Committee to Review Law Enforcement’s Policies.”*

76. *Sam Levin, “ACLU finds social media site gave data to company tracking black protesters,” the Guardian, October 11, 2016, available at https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter.*

77. *All descriptions of FBI access to state DMV photo databases described in this section are attributable to the research found in Claire Garvie et al., “The Perpetual Lineup.” All data on number of individuals included in state DMV databases are based on the listing of number of licensed drivers in each state according to “2015 State Statistical Abstracts,” Federal Highway Administration Policy and Government Affairs Office of Highway Policy Information, 2015, https://www.fhwa.dot.gov/policyinformation/statistics/abstracts/2015/.*

78. *Maryland, H.B. 1148 (2017), http://mgaleg.maryland.gov/2017RS/bills/hb/hb1148f.pdf.*

79. *Oregon, H.B. 2571 (2015), https://olis.leg.state.or.us/liz/2015R1/Downloads/MeasureDocument/HB2571/A-Engrossed.*

80. *Rhode Island, H. 5521 (2017), https://legiscan.com/RI/drafts/H5521/2017.*

81. *California, S.B. 178 (2015), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178.*

82. *Illinois, S.B. 2808 (2014), http://ilga.gov/legislation/publicacts/98/PDF/098-1104.pdf.*

83. *Peter Cihon, “Status of Location Privacy Legislation in the States.”*

84. *Indiana, HEA 1009 (2014), http://iga.in.gov/static-documents/5/3/4/4/5344c8fc/HB1009.06.ENRH.pdf.*

85. *Maine, S.P. 157 (2013), http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0157&item=6&snum=126.*

86. *Minnesota, S.F. 2466 (2014), https://www.revisor.mn.gov/bills/text.php?number=SF2466&version=3&session=ls88&session_year=2014&session_number=0&format=pdf.*

87. *Montana, H.B. 603 (2013), http://leg.mt.gov/bills/2013/billpdf/HB0603.pdf.*

88. *New Hampshire, H.B. 468 (2015), http://www.gencourt.state.nh.us/legislation/2015/HB0468.pdf.*

89. *Utah, H.B. 128 (2014), http://le.utah.gov/~2014/bills/hbillenr/HB0128.pdf.*

90. *Virginia, H. 1408 (2015), http://leg1.state.va.us/cgi-bin/legp504.exe?151+ful+CHAP0043+pdf.*

91. *Washington, H.B. 1440 (2015), http://lawfilesext.leg.wa.gov/biennium/2015-16/Pdf/Bills/Session%20Laws/House/1440-S.SL.pdf.*

Jake Laperruque, Contributor

Jake Laperruque is Senior Counsel at The Constitution Project, where he works on issues of government surveillance, national security and defending privacy rights in the digital age. Prior to joining TCP, Jake was a fellow at New America's Open Technology Institute and at the Center for Democracy and Technology. He previously served as a law clerk for Senator Al Franken on the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, and as a policy fellow for Senator Robert Menendez. He is a graduate of Washington University in St. Louis and Harvard Law School. You can follow him at @jakelaperruque on Twitter.