The Heritage Foundation

LEGAL MEMORANDUM

No. 274 | OCTOBER 30, 2020

EDWIN MEESE III CENTER FOR LEGAL & JUDICIAL STUDIES

Addressing Legitimate Concerns About Government Use of Facial Recognition Technologies

Brian E. Finch

KEY TAKEAWAYS

The capabilities of facial recognition systems have improved dramatically, especially by reducing the possibility of individual misidentification.

The U.S. should set testing benchmarks for facial recognition systems so public-sector users can purchase systems unlikely to enable discrimination.

Updated encryption standards should be applied to facial recognition databases to make them less vulnerable to theft by foreign adversaries.

The adoption of facial recognition technology (FRT) by federal and state government agencies—specifically, by law enforcement for identifying unknown individuals suspected of committing crimes—has generated a particularly heated debate about whether its potential benefits are outweighed by concerns over its potential for misuse and abuse. Some states and cities, including, most recently, Portland, Oregon, have gone so far as to ban the use of FRTs by government agencies.[1]

Advocates for the government use of FRT argue that it represents a significant leap forward for law enforcement's crime surveillance and investigatory purposes thanks to its unique identification and verification capabilities. Privacy advocates, on the other hand, have expressed vehement opposition to law enforcement's use of FRTs. They argue that FRTs will enable an expansion of an abusive surveillance state

and, further, that they are an inherently flawed and discriminatory tool that inevitably discriminates against minorities and historically repressed communities.[2] Such concerns have become significant enough that congressional legislation has been introduced that would ban the use of FRTs by the federal government.[3]

High-profile early adoption of FRTs by repressive regimes has no doubt played a role in magnifying some of these concerns. The most notable example has been the widespread use of FRTs by the People's Republic of China as an integral part of an omnipresent electronic surveillance network it utilizes to track and monitor its citizens—including for the rapid suppression of dissent.

Critics consider China's authoritarian use of FRTs as one of many reasons to oppose their use by American law enforcement agencies. Such concerns, along with questionable enhancements to FRTs through the use of technologies from companies like Clearview AI, have recently led Amazon and Microsoft to suspend sales of such systems to domestic police departments.[4] IBM has gone even further, choosing to completely exit the facial recognition market due to its fears that the technology could lead to widespread "violations of basic human rights and freedom."[5]

While fears about the potential for abuse are not unfounded, they can be significantly mitigated through innovation and policy decisions. In particular, testing already conducted by federal agencies on FRTs can be used to minimize any possible bias in algorithms.

Another much less appreciated, but perhaps just as worrying, concern about FRTs is that vulnerabilities in the FRT infrastructure make them a particularly ripe espionage target for foreign governments. Should that be the case, greater care should be paid to emerging cybersecurity concerns related to facial recognition systems. As discussed in this *Legal Memorandum*, both stronger privacy and security controls are needed on FRTs before they could be widely adopted by U.S. government agencies.

Overview of FRTs and Government Use for Identification Purposes

To begin, while the use of FRTs in both commercial and government settings raises many similar privacy and security concerns, this paper focuses solely on government use of FRTs. Therefore, this paper should not be read as offering any recommendations about commercial uses of facial recognition systems.

FRT Types. Any FRT follows three basic steps in its operation. First, during the *face detection* step, a computer algorithm determines whether the captured facial image is human.[6] Once a human face has been successfully detected, the software moves to the second step, *feature extraction*, where specific facial features such as the nose and eyes are captured and measured.[7]

The third and final step is "*facial recognition*" or "template matching" process, wherein the software compares the measurements from the captured image and compares it with known faces stored in specific databases. Facial recognition systems utilizing the template methodology use computer algorithms to pick out specific, distinctive details about a person's face that have been converted into mathematical representation.[8]

One-to-One Matching. That template-matching system underpins the two most common uses of FRTs. One system is known as is "1:1 matching" or "verification." This system is most familiar to the public, as it is the system used for security tools such as face "unlocking" of mobile devices or biometric credential authorization for passports. Much like its name, one-to-one matching uses the FRT of that photo or presented face to see if it matches a different photo of the same person stored in a database or on a credential.[9] Other uses could potentially include identifying individuals who are at risk of developing a genetically inherited disorder or measuring their general wellness.[10]

One-to-Many Matching. The other commonly used facial recognition system, and the one that is the source of most of the worries examined in this paper, is known as "one-to-many," "1:N," or facial recognition "identification" system. FRTs equipped with one-to-many algorithms are used to compare a captured image of an unknown/unidentified person against a database of photographs of previously identified persons (such as through mugshots or other verified photographs). The system will then produce a number of possible "matches" to the unknown person.[11]

One-to-many searches are conducted using algorithms designed to return photos or a group of photos based on a "similarity score" set either by the user or the algorithm developer. If none of the matches meets or exceeds that preset similarity score, the algorithm will not return any images as a potential or actual match.

Performance of one-to-many algorithms is generally measured by two metrics. The first is what is known as the accuracy rate, which is defined as the rate at which the "matching" image should be returned as a candidate. Algorithm developers and tests will also calculate the failure rate, the rate at which a matching image is not returned despite being in the data set.[12] Other measurements of performance are "false positive" and "false negative" rates, which will be discussed below.

Government FRT Identification Programs

In order to better put the concerns associated with U.S. law enforcement use of FRTs in context, especially with respect to one-to-many/identification searches, this section will briefly review typical government use of FRTs.

The most well-known federal law enforcement FRT identification platform is the Federal Bureau of Investigation's Next Generation Identification-Interstate Photo System (NGI-IPS). The NGI-IPS contains criminal mug shots and civil photos submitted with ten-print fingerprints and offers a facial recognition search capability to law enforcement agencies trying to solve crimes.[13]

Within the NGI-IPS, photos are separated into two categories: the Criminal Identity Group, which consists of mug shots associated with arrests, and the Civil Identity Group, which contains photos of applicants, employees, licensees, and persons in positions of public trust.[14] Photos contained in the Civil Identity Group are not disseminated to other law enforcement groups and are not searched by or against photos in the Criminal Identity Group.

The only exception to the non-searching and non-dissemination Civil Identity Group photos is if the identified person has a photo in both the Civil and Criminal Identity Groups. In such cases, a photo originally submitted for Civil Identity Group purposes will also be searched when a Criminal Identity Group search is conducted.[15]

The NGI-IPS is used by the FBI and select state and local law enforcement agencies. Prior to using the NGI-IPS, state and local law enforcement officials must: (1) complete facial recognition training, and (2) agree that the returned photos are for investigative lead purposes only and not a definitive positive identification of the perpetrator of a crime.[16]

The NGI-IPS uses an automated process to return between two and 50 images, called "candidate photos," from the database that are submitted to the requesting agency for manual review and further investigation.[17] The FBI has its own dedicated unit, the Facial Analysis, Comparison, and Evaluation Services Unit to conduct the manual review of images.

It has been estimated that up to one in four local law enforcement agencies have access to some form of facial recognition system.[18] The New York City Police Department (NYPD), for instance, has used facial recognition systems for several years. Much like with the FBI's requirements, NYPD officers must manually review returned candidate photos and are prohibited from using facial recognition matching alone to establish probable cause to arrest anyone based on that match without first conducting additional investigation to verify their suspicions.[19]

Legal Status of Facial Recognition Systems for Identification Purposes

One commonly asked question is whether there are any legal restrictions that govern the use of FRTs by government agencies. Most scholars believe that the use of FRTs by law enforcement agencies is not limited by the Fourth Amendment.

As Professor Andrew Guthrie Ferguson, a noted Fourth Amendment scholar, explains:

> Generalized face surveillance involves monitoring public places or third-party image sets using facial surveillance technologies to match faces with a pre-populated list of face images held by the government. Currently, no federal law prohibits this type of generalized surveillance using facial recognition technology.... The Fourth Amendment has little to say directly about the digital or human recognition of faces.[20]

Ferguson adds that the pertinent question a court would ask for purposes of determining whether the Fourth Amendment applies would be whether the technology violates an accused's "reasonable expectation of privacy."[21] However, as Ferguson and others have noted, prior to the digital age, the Supreme Court held that no person could "reasonably expect that his face will be a mystery to the world."[22] Some scholars diverge from that line of reasoning, arguing that anonymity—not privacy—is the fundamental right being trampled upon by FRTs.[23]

That does not exclude, of course, the Supreme Court revisiting this issue in a future case, as they have done with other issues that were generally considered settled before the digital age.[24] Indeed, some legal scholars argue that the judicial silence on the legality of FRTs is more likely due to the fact that law enforcement agencies rarely reveal their use during a criminal investigation than to any generalized judicial acceptance of them.[25]

As the law enforcement use of FRTs becomes more widely acknowledged, that could prompt legal challenges that might cause courts to re-examine the issue and establish possible limits on its use. Fearing that "without appropriate safeguards, face surveillance can become a generalized dragnet where every person becomes the target of government monitoring,"[26] some local jurisdictions are not waiting for courts to act. Driven by such concerns, as well as worries about the discriminatory impact of the use of FRTs, jurisdictions such as San Francisco and Oakland have stepped into the void and limited or even banned entirely government use of facial recognition software.

A complete ban has gained some traction amongst certain privacy scholars as they believe the overall negatives of FRTs outweigh any potential benefits.[27] Congressional privacy advocates have also proposed a complete ban on FRTs at the federal level, saying that Congress "must ban facial recognition until we have confidence that it doesn't exacerbate racism and violate the privacy of American citizens."[28] Others have limited or banned the use of FRTs in specific locations, such as public schools.[29]

Concerns About Mistaken FRT Results Can Be Mitigated Through Policy and Legal Measures

As with any cutting edge, innovative technology, there have been issues with the accuracy of FRTs. As noted above, some of these issues relate to generalized privacy concerns related to the implementation of automated surveillance systems. Other concerns are grounded in the maturity of FRTs—specifically, continuing concerns about whether the systems are developed enough to sufficiently minimize the possibility of misidentification. As discussed below, concerns about misidentification are legitimate, but also can be mitigated through policy and legal measures.

One-to-Many FRT False-Positive Issues

As with any search—whether conducted by humans or computerized by algorithms—the possibility of mistakes exists. For FRTs, the two most relevant errors are classified as either the "false positive" rate or the "false negative" rate.[30]

False Negatives. A false negative occurs when an algorithm fails to return a matching image despite being in the defined set.[31] Should such an error occur, for example, during a one-to-one verification attempt, an individual might be improperly denied access to a system or technology to which he or she is, in fact, an authorized user. The rate of false negatives varies greatly among proprietary algorithms.

False Positives. Of greater worry to civil libertarians are "false positive" rates. A "false positive" occurs when the image of one individual is matched to the biometric characteristics of an entirely different person, resulting in a misidentification.[32] The consequences of a false positive in a one-to-many system can be especially serious, including leading to the mistaken arrest of an innocent person based largely, if not entirely, on the misidentification.

Important to note is that there are many possible reasons for a false negative or false positive, the age of the images being searched against;

the environment (background, lighting conditions, camera distance, etc.) in which the photograph was taken; and the optical characteristics of the cameras being used.[33]

The most well-known effort to measure false negative and false positive rates is the National Institute of Standards and Technologies (NIST) Face Recognition Vendor Testing Program (FRVT).[34] Since the FRVT began in 2000, it has tested hundreds of algorithms, measuring false negative rates, for instance, anywhere between 0.03 percent to over 90 percent.[35]

According to NIST, during the past 10 years, the FRVT has measured "massive gains in accuracy" of FRTs thanks to the use of newer facial recognition techniques and deep convolutional neural networks.[36] The NIST FRVT has also revealed, unfortunately, that the accuracy of various FRT algorithms can drop significantly when photos of non-white males are being analyzed. The NIST was able to identify that issue as FRVT data captured the accuracy of facial recognition algorithms for demographic groups defined by sex, age, and race or country of birth, for both one-to-one verification algorithms and one-to-many identification search algorithms.[37] When those more discrete sets of data were analyzed, the NIST reported that the general statement about "massive" accuracy gains actually masked significant concerns about higher false positive rates for certain demographics, particularly for one-to-many identification search algorithms. Specifically, the NIST found that there was a higher false-positive rate in women and African-Americans (especially African-American women) in most algorithms.[38]

Discriminatory False Positives Reduced Through Policy Changes

Not surprisingly, these results have been cited as evidence that the higher rate of one-to-many FRT false positives means that the technology would enable discriminatory behavioral patterns, which many believe are already widespread among American law enforcement agencies. The NIST itself has noted, however, that the study did not conclude that false positives are a problem inherent in one-to-one/identification FRT algorithms. To wit:

> [T]he study found that some one-to-many algorithms gave similar false positive rates across these specific demographics. Some of the most accurate algorithms fell into this group. This last point underscores one overall message of the report: Different algorithms perform differently. Indeed all of our FRVT reports note wide variations in recognition accuracy across algorithms, and an important result from the demographics study is that demographic effects are smaller with more accurate algorithms.[39]

The NIST's point could not be any clearer: FRTs are not always biased against minorities or sub-demographics. Far from it. Instead, a number of FRT algorithms have very similar—and very small—false-positive rates regardless of the demographic involved. More specifically, the NIST FVRT program has demonstrated effectiveness in identifying FRT algorithms that produce similarly low one-to-many false positive rates regardless of the demographic involved.

That distinction is critical for two reasons. First, it refutes a linchpin argument of many FRT opponents, namely that because the technology is inherently discriminatory against minorities, its use will necessarily result in higher mistaken arrests or misidentifications of minority subjects for activities they had nothing to do with. The use of fully vetted FRTs to ensure that they have similar false-positive rates across all demographics will help rebut arguments that a minority was identified in a FRT search solely because the algorithm used was discriminatory. Given the existing ability of the FVRT program to generate those results, federal procurements of FRTs and federal grant funds being spent on FRTs should only be allowed when FVRT results indicate that the algorithm used in the FRT has a false-positive rate below a certain threshold that minimizes, if not eliminates, concerns about FRTs producing inequitable resorts for minorities.

Additionally, any federal one-to-many FRT program should be modeled on the FBI's program, including its mandatory training requirements. As previously noted, the FBI's program generates a pool of results (anywhere from two to 50), which then must be manually reviewed by trained individuals to see if they are, in fact, a match for the unknown subject. And such results must be corroborated by the results of additional investigation. Statutory options exist to further limit false positive concerns in identification searches

Again, some jurisdictions have been more proactive than others when it comes to addressing concerns about the potential discriminatory impact of FRTs by regulating—not eliminating—their use by law enforcement agencies to solve crimes. For example, in March 2020, the state of Washington enacted a law allowing state and local law enforcement agencies to use FRTs subject to very specific controls.[40]

The new law requires state or local government agencies to notify the public of their intent to buy or use facial recognition tools before doing so. As part of that public notification requirement, agencies are obligated to issue an "accountability report" that identifies the proposed use of the FRT and the data it will generate, detailing:

- False positive rates of the FRT;
- Data security measures that will be used to protect the FRT; and
- Any agency procedures for testing the tools and receiving feedback.

The new law also mandates "meaningful human review," described as human review by someone who has undergone training on the use of FRTs prior to any final determination on actions to be taken when the use of facial recognition software produces "legal effects or similarly significant effects concerning individuals."

Another critical component of the law is that, absent exigent circumstances, it will require government agencies to obtain a warrant prior to running facial recognition scans when conducting "real-time or near real-time identification."[41] The law also prohibits the use of the results of a facial recognition system "as the sole basis to establish probable cause in a criminal investigation."[42] Instead, the results of a FRT search can only be used in conjunction with other information and evidence lawfully obtained by a law enforcement officer to establish probable cause in a criminal investigation.[43]

The key components of the Washington law, including requiring full understanding of the effectiveness of the FRT as well as limiting its use to specific circumstances, demonstrate how legislation can further minimize legitimate privacy and discriminatory concerns. Requiring a warrant when "real-time or near real-time identification" is conducted should ease worries about the government employing the "unblinking eye" of FRTs to constantly track an individual's movements and whereabouts for any reason.

Other states with similar concerns about the use of FRTs may wish to pass laws modeled on Washington state's law. The key conclusion is that while FRT privacy and discrimination concerns are real, they are hardly insurmountable.

External Threats: Foreign Government Surveillance and Collection

Another very real, but less frequently addressed, concern is the use of FRTs in the area of national security. Could FRT databases be penetrated via cyberattack and used to feed foreign government surveillance databases?

Given current trends, especially with respect to Chinese efforts to hack into American surveillance systems and amass biometric information on American citizens, greater attention should be paid to ensuring that current security

controls on facial recognition databases are adequate. A brief review reveals that current systems are, in fact, vulnerable to infiltration and exfiltration through foreign espionage efforts, with the result being that the most pressing threat to the privacy of Americans from facial recognition surveillance systems may be the theft and misuse of the images by foreign governments.

To begin, China and other foreign governments have a consistent pattern of stealing the biometric and personal data of Americans through cyberespionage. China, for instance, stole well over 5 million biometric fingerprint records when it successfully hacked into the U.S. Office of Personnel Management in 2015.[44] Chinese hackers were also implicated in the theft of nearly 80 million health records maintained by U.S. health insurance companies.[45] Other records, such as photos of travelers, have been stolen from U.S. law enforcement databases.[46]

In the most recent incident, nearly 184,000 biometric images of travelers were stolen via a hack conducted against a U.S. government contractor, with a small number subsequently being posted on the "dark web."[47] Notably, the biometric images were already unencrypted when the government contractor downloaded them, making it all the easier for the hacker to publish them.[48] And while not strictly in the category of biometric data, Russian hackers recently stole all manner of research related to the COVID-19 pandemic, including information critical to the development of vaccines.[49]

Compounding the potential damage from such biometric thefts is the fact that few laws have been written or amended to increase security over what is obviously high-value data. For instance, while Washington State's new facial recognition privacy law rigorously details how facial recognition data can be shared or used, it offers few details on the measures needed to protect that information. It states only:

> Data security measures applicable to the facial recognition service including how data collected using the facial recognition service will be securely stored and accessed.[50]

The general lack of attention to security—and, more specifically, the lack of encryption for facial recognition images resting in a database—is worrisome. Even basic privacy standards for biometrics, such as IEEE P2410 (Institute of Electrical and Electronics Engineers' Standard for Biometric Privacy), only contemplated biometric matching (including facial recognition) being conducted using unencrypted data. In other words, without encryption, the photos contained in FRT databases could be put to use by adversaries as soon as they are stolen.

Leaving U.S. facial recognition repositories largely unprotected creates a tempting target for international cyber-recidivists like China, which maintains the world's largest surveillance camera and facial recognition database.[51] Starting several years ago as a program to monitor and suppress its Uighur Muslim minority,[52] China now has over 620 million facial recognition software-equipped surveillance cameras inside its borders[53] and is using them as an integral part of its program designed to track and rank its citizens nationwide.[54] China has even used the facial recognition network in its campaign to control the COVID-19 outbreak, specifically to identify Chinese citizens with signs of infection or who are identified as having violated quarantine rules.[55]

Beijing has consistently sought to increase the size of its facial recognition database, including by capturing images of Chinese citizens overseas, as well as foreign nationals. Popular social media tools tied to Chinese ownership, for instance, have been identified as potential sources of espionage, based on information showing that Beijing pressured those companies to share the information and images they collect with government authorities.[56] Evidence also suggests that Chinese-made surveillance cameras are prone to hacking by the Chinese government,[57] which would enable Beijing to use those cameras for espionage purposes, such as identifying and tracking specific individuals in foreign countries.[58]

These alarming trends raise the specter that as U.S.-based government agencies and private entities build larger facial recognition databases, those databases will, in turn, be used to enrich China's facial recognition system or be used for other nefarious purposes by foreign governments that are able to successfully extract that information.

A Chinese database stocked with tens of millions of images of American citizens would present an existential threat to American security and privacy, since Americans living or traveling abroad could easily be tracked and identified (or misidentified) by China and the myriad of countries who have purchased its surveillance systems. Further, given China's heavy investment in disruptive cyberattack capabilities, the possibility exists as well that China could use the stolen high-quality images to spread disinformation or even create malicious false information about Americans at home and abroad.

Policy Recommendations

Widespread adoption of FRT by U.S. law enforcement agencies could indeed pose both discriminatory and security threats. NIST testing has demonstrated that some FRT algorithms generate unacceptable false

positive rates for specific demographics. Further, existing security standards leave facial recognition databases uniquely vulnerable to exploitation via cyberattack by foreign governments seeking to increase the size of their own facial recognition databases in order to improve their own surveillance networks.

While the potential benefits from the use of FRTs are great—especially to assist law enforcement agencies to solve crimes—such concerns and threats should be taken seriously, and concrete steps should be taken to minimize the risks involved including the following:

- **Require the NIST to provide false-positive rates for racial, ethnic, and gender groups when testing results for identification (1:N) algorithms.** The NIST testing has shown that FRT false-positive rates in one-to-many uses can greatly vary when separated by racial, ethnic, and gender groups. NIST should continue to produce those results through its FVRT program as these results will be useful for both acquisition purposes and increasing the credibility and acceptability of the use of facial recognition systems within prescribed guidelines with the general public.

- **Require maximum acceptable false-positive rates across racial, ethnic, and gender groups for federal procurement of 1:N algorithms.** Recognizing that FRTs have immaterial differences in false positive rates across minority groups, the federal government should establish maximum acceptable false-positive rates across those same minority groups for federal acquisition purposes. Doing so will significantly limit concerns that federal law enforcement use of FRTs will only serve to enable discrimination against minority groups.

- **Adopt legislation addressing government use of FRTs that focuses on limiting, not prohibiting, their use and on educating the public about those limitations and their legitimate uses.** Codifying limits on when and how FRTs are used will go a long way to building further confidence that the systems are being used for legitimate, equitable law enforcement purposes. Washington State's facial recognition law can serve as a valuable model for future legislation, particularly given its mix of technological and policy requirements.

- **Require increased encryption on government facial recognition systems.** As it currently stands, there is no uniform encryption

requirement for government FRT algorithms or systems in general. That should change, including by potentially adopting updated biometric privacy standards from IEEE for federal, state, and local facial recognition systems. The existing standard is currently being revised, and should include strong encryption requirements for biometric data, including facial recognition data at rest, in use, or in transit.

- **Share threat information with industry.** Given repeated large-scale thefts of biometric data and personal information by foreign adversaries, American businesses should be kept as informed as possible about threats to identity data they may possess or collect. Since the government is likely to have the best and most up-to-date information about such espionage efforts, U.S. cybersecurity officials should make sure to include threat intelligence information about attacks on or vulnerabilities related to facial recognition systems to the American private sector.

Conclusion

Facial recognition technologies can materially increase the ability of law enforcement agencies to timely identify suspects. Still, legitimate worries about misidentification and improper use by law enforcement must be addressed as part of any effort to increase the use of these technologies. By requiring rigorous testing and training, the federal government can significantly allay those concerns, especially when combined with increased cybersecurity measures. With that combination, American citizens can have confidence in the accuracy and effectiveness of FRTs when used by government agencies.

Brian E. Finch is Visiting Legal Fellow in the Edwin Meese III Center for Legal and Judicial Studies, of the Institute for Constitutional Government, at The Heritage Foundation.

Endnotes

1. Courtney Linder, "Why Portland Just Passed the Strictest Facial Recognition Ban in the U.S.," *Popular Mechanics*, September 12, 2020, https://www.popularmechanics.com/technology/security/a33982818/portland-facial-recognition-ban/ (accessed October 19, 2020).
2. "Street-Level Surveillance: Face Recognition," Electronic Frontier Foundation, October 24, 2017, https://www.eff.org/pages/face-recognition (accessed June 15, 2020)
3. Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong., 2nd Sess., https://www.congress.gov/bill/116th-congress/senate-bill/4084/text (accessed October 19, 2020).
4. Ari Levy, "Microsoft Says It Won't Sell Facial Recognition Software to Police Until There's a National Law 'Grounded in Human Rights,'" CNBC, June 11, 2020, https://www.cnbc.com/2020/06/11/microsoft-says-will-not-sell-facial-recognition-software-to-police.html (accessed June 17, 2020).
5. David Meyer, "IBM Pulls Out of Facial Recognition, Fearing Racial Profiling and Mass Surveillance," *Fortune Magazine*, June 9, 2020, https://fortune.com/2020/06/09/george-floyd-ibm-exits-facial-recognition-bias-human-rights/ (accessed June 17, 2020).
6. Ibid.
7. Ibid.
8. Kristine Hamann and Rachel Smith, "Facial Recognition Technology: Where Will It Take Us?" *Criminal Justice*, Vol. 24, No. 1 (Spring 2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ (accessed May 26, 2020)
9. Charles H. Romine, "Facial Recognition Technology," testimony before Committee on Homeland Security, U.S. House of Representatives, February 6, 2020, https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0 (accessed May 27, 2020).
10. Seema Mohapatra, "Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation," *Pepperdine Law Review*, Vol. 43, No. 4 (June 2, 2016), https://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=2416&context=plr (accessed Sept. 23, 2020).
11. Romine, "Facial Recognition Technology."
12. "Face Facts: Dispelling Common Myths About Facial Recognition Technology," Security Industry Association, June 2019, https://www.securityindustry.org/wp-content/uploads/2019/06/facial-recognition-20193.pdf (accessed May 25, 2020).
13. Federal Bureau of Investigation, "Privacy Impact Assessment For The Next Generation Identification-Interstate Photo System," October 29, 2019, https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view#:~:text=This%20Privacy%20Impact%20Assessment%20(PIA,to%20the%20FBI%20for%20authorized (accessed May 25, 2020).
14. Ibid.
15. Ibid.
16. Kimberly J. Del Greco, "Facial Recognition Technology: Ensuring Transparency in Government Use," testimony before the House Oversight and Government Reform Committee, U.S. House of Representatives, June 4, 2019, https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use (accessed May 30, 2020).
17. Ibid.
18. Shirin Ghaffary, "How to Avoid a Dystopian Future of Facial Recognition in Law Enforcement," Vox, December 10, 2019, https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation (accessed May 25, 2020).
19. New York Police Department, "Patrol Guide: Facial Recognition," https://www1.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf (accessed Sept. 15, 2020)
20. Andrew Guthrie Ferguson, "Written Testimony of Professor Andrew Guthrie Ferguson Before the House of Representatives Committee on Oversight and Reform Hearing On: Facial Recognition Technology: (Part 1) Its Impact on our Civil Rights and Liberties," testimony before the Committee on Oversight and Government Reform, U.S. House of Representatives, May 22, 2019, https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-FergusonA-20190522.pdf (accessed May 27, 2020).
21. Ibid.
22. *U.S. v. Dionisio*, 410 U.S. 1 (1973).
23. Sharon Nakar and and Dov Greenbaum, "Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy," Boston University School of Law *Journal of Science and Technology*, Vol. 23, Issue 1 (Winter 2017), https://www.bu.edu/jostl/archives/vol-23-1-winter-2017/ (accessed Sept 26, 2020).
24. See, for instance, *Riley v. California*, 573 U.S. 373 (2014) (holding that the warrantless search and seizure of digital contents of a cell phone during an arrest is unconstitutional), and *Carpenter v. United States*, No. 16-402, 585 U.S. _____ (2018) (holding that the Fourth Amendment requires the government to obtain a search warrant in order to access records containing the physical location of cell phones).

25. Neema Singh Guliani, "Statement on Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties," testimony before Committee on Oversight and Government Reform, U.S. House of Representatives, May 22, 2019, https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-GulianiN-20190522.pdf (accessed May 27, 2020).
26. Ferguson, "Written Testimony of Professor Andrew Guthrie Ferguson Before the House of Representatives Committee on Oversight and Reform Hearing On: Facial Recognition Technology: (Part 1) Its Impact on our Civil Rights and Liberties."
27. "Professor Woodrow Hartzog Calls for a Ban on Facial Recognition Technology in New Publication," Northeastern University, April 14, 2020, https://www.northeastern.edu/clic/woodrow-hartzog-calls-for-a-ban-on-facial-recognition-technology/ (accessed Sept. 16, 2020).
28. "Senators Markey and Merkley, and Reps. Jayapal, Pressley, To Introduce Legislation To Ban Government Use of Facial Recognition, Other Biometric Technology," Office of Senator Edward Markey, June 25, 2020, https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology (accessed September 15, 2020).
29. Chris Mills Rodrigo, "New York Legislature Bans Use of Facial Recognition Technology in Schools," *The Hill*, July 23, 2020, https://thehill.com/policy/technology/508809-new-york-legislature-bans-use-of-facial-recognition-technology-in-schools (accessed August 19, 2020).
30. "Street-Level Surveillance."
31. "Face Facts: Dispelling Common Myths About Facial Recognition Technology."
32. Hamann and Smith, "Facial Recognition Technology: Where Will It Take Us?"
33. Lucas D. Introna and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, New York University Center For Catastrophe Preparedness and Response, https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf (accessed June 15, 2020).
34. Romine, "Facial Recognition Technology."
35. National Institute of Standards and Technology, "FVRT 1:1 Verification," September 10, 2020, https://pages.nist.gov/frvt/html/frvt11.html#overview (accessed Sept. 15, 2020).
36. Ibid.
37. National Institute of Standards and Technology, "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," December 19, 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software (accessed May 24, 2020).
38. Ibid.
39. Romine, "Facial Recognition Technology."
40. Washington State Legislature, S.B. 6280, 2019–2020 Sess., https://app.leg.wa.gov/billsummary?BillNumber=6280&Initiative=false&Year=2019#documentSection (accessed October 20, 2020).
41. State of Washington, Engrossed Substitute Senate Bill 6280: Facial Recognition, 66th Legislature, 2020 Reg. Sess., http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Session%20Laws/Senate/6280-S.SL.pdf?q=20200828130542 (accessed October 19, 2020).
42. Ibid.
43. Ibid.
44. Andy Greenberg, "OPM Now Admits 5.6m Feds' Fingerprints Were Stolen By Hackers," *Wired*, September 23, 2015, https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/ (accessed May 27, 2020).
45. Mackenzie Garraty, "U.S. Indicts Chinese Hacker for Exposing 80M Anthem Patient Records," Beckers Health Care, May 10, 2019, https://www.beckershospitalreview.com/cybersecurity/us-indicts-chinese-hacker-for-exposing-80m-anthem-patient-records.html (accessed May 30, 2020).
46. Drew Harwell and Geoffrey A. Fowler, "U.S. Customs and Border Protection Says Photos of Travelers Were Taken In A Data Breach," *Washington Post*, June 10, 2019, https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/ (accessed September 15, 2020).
47. Matthew Gault, "DHS Admits Facial Recognition Photos Were Hacked, Released on Dark Web," Vice, September 24, 2020, https://www.vice.com/en/article/m7jzbb/dhs-admits-facial-recognition-photos-were-hacked-released-on-dark-web (accessed Sept. 27, 2020).
48. U.S. Department of Homeland Security, "Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot," Office of the Inspector General, September 21, 2020, https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf (accessed September 27, 2020).
49. Julian E. Barnes, "Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say," *The New York Times*, July 16, 2020, https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html (accessed August 23, 2020).
50. State of Washington, Engrossed Substitute Senate Bill 6280: Facial Recognition.
51. Lauren Dudley, "China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash," *The Diplomat*, March 7, 2020, https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/ (accessed August 24, 2020).

52. "China Is Now Using Facial Recognition Cameras to Monitor Uighur Muslims Across the Country, Report Claims," *Daily Mail*, April 15, 2019, https://www.dailymail.co.uk/news/article-6924349/China-using-AI-identify-Uighurs-China-NYT.html (accessed May 26, 2020).
53. Dudley, "China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash."
54. Bradford Betz, "What Is China's Social Credit System?" Fox News, May 3, 2020, https://www.foxnews.com/world/what-is-china-social-credit-system (accessed May 27, 2020).
55. Cate Cadell, "China's Coronavirus Campaign Offers Glimpse Into Surveillance System," Reuters, May 26, 2020, https://www.reuters.com/article/us-health-coronavirus-china-surveillance/chinas-coronavirus-campaign-offers-glimpse-into-surveillance-system-idUSKBN2320LZ (accessed June 15, 2020).
56. Rebecca Jennings, "What's Going on With TikTok, China, and the U.S. Government?" Vox, December 16, 2019, https://www.vox.com/open-sourced/2019/12/16/21013048/tiktok-china-national-security-investigation (accessed May 25, 2020).
57. Zak Doffman, "Warning As Millions Of Chinese-Made Cameras Can Be Hacked To Spy On Users: Report," *Forbes*, August 3, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/#322a4b5c6bf2 (accessed May 27, 2020).
58. "U.S. Government Ban of Dahua, Hikvision, Huawei Takes Effect Now," August 13, 2019, https://ipvm.com/reports/aug-13-2019 (accessed May 27, 2020)