STATEMENT OF

NEEMA SINGH GULIANI
SENIOR LEGISLATIVE COUNSEL, WASHINGTON LEGISLATIVE OFFICE
AMERICAN CIVIL LIBERTIES UNION

For a Hearing on:

"Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties."

Before

House Oversight and Reform Committee

May 22, 2019

For further information, please contact Neema Singh Guliani, Senior Legislative Counsel, at nguliani@aclu.org.

Chairman Cummings, Ranking Member Jordan, and Members of the Committee,

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU)[i] and for holding this hearing on, "Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties."

Across the country, people continue to be harmed by government use of face recognition, which in many cases is being actively sold and marketed by poorly regulated private companies. In Colorado, Steven Talley was held for nearly two months after being wrongly arrested by police based on face recognition technology that mistakenly identified him as a suspect in a bank robbery surveillance video. [ii] In Baltimore, the police reportedly used face recognition on photos posted on social media to identify individuals at a rally against police violence, risking chilling First Amendment activity.[iii] A Brown University student from Maryland falsely identified through use of a face recognition program by foreign authorities as being involved in the Sri Lankan Easter bombings had her photo plastered on the internet, leading to death threats.[iv] And, in Florida, key details of the reliability of a face recognition algorithm continue to be withheld from Willie Lynch, who was arrested and convicted of a $50 dollar drug crime based on a low confidence match of a poor quality photo taken by undercover police. [v]

State and local governments, shareholders, and organizations across the country are working to halt the irresponsible expansion of this dangerous technology and prevent further harm. The San Francisco Board of Supervisors voted overwhelmingly to ban the use of face recognition by city departments,[vi] while states like Massachusetts and Washington have introduced legislation that would put in place a moratorium on law enforcement use.[vii] Thirteen localities – including Yellow Springs, Ohio and Nashville, Tennessee – have passed laws requiring legislative approval and public impact assessments before new surveillance technologies, like face recognition, can be deployed.[viii] And earlier this month, Amazon shareholders won the right to vote on resolutions – overcoming company objections filed with the Securities and Exchange Commission – over whether Amazon should stop selling this technology to the government or further study the human rights impacts.[ix]

Despite these efforts, additional Congressional action in this arena is sorely needed. By giving police the capability to identify individuals in real-time or reconstruct their every movement from photos or videos, face recognition can create a near constant surveillance state that threatens our core constitutional values. Already, many existing uses of the technology violate the Fourth Amendment. These harms fall disproportionately on communities of color and immigrant communities, who are already overpoliced and more likely to be stopped, arrested, or have force wrongly used against them. Thus, the ACLU urges the Committee to:

1) **Take steps to halt the use of face recognition for law enforcement and immigration enforcement purposes until Congress passes a law dictating what, if any, uses are permissible and ensures that individuals' rights can be protected;**
2) **Fully utilize its oversight powers to make public information regarding how federal agencies, including the FBI and ICE, are using face recognition; whether they are**

complying with their constitutional notice obligations; what policies are in place to prevent rights abuses; and whether their systems are accurate; and

3) **Investigate companies, like Amazon and Microsoft, that sell face recognition for law enforcement use and without taking adequate responsibility or enforcing sufficient safeguards to prevent abuse.**

I. Use of face recognition threatens to create a near constant surveillance state, undermining core constitutional values

Advances in face recognition threaten to create an almost Orwellian surveillance state, where individuals cannot evade constant surveillance and tracking. Companies are now marketing face recognition that is not only capable of identifying individuals from photographs, but also able to surreptitiously track individuals or reconstruct their past movements from videos. According to some estimates, there are 50 million surveillance cameras throughout the United States - and a growing number of jurisdictions where police use body worn cameras.[x] Video cameras are even being integrated into everyday objects, like doorbells. As technology develops, the increased number of cameras combined with face recognition may give the government the capability to monitor citizens' every movement, without their knowledge or consent.

These concerns are all the more striking given the threat that face recognition poses to First Amendment expression. As Justice Sotomayor pointed out in *Jones*, "Awareness that the Government may be watching chills associational and expressive freedoms."[xi] We should all have the right to take part in everyday activities – be it sitting in a park or attending a political rally – anonymously and without fear of government intrusion. Face recognition threatens this right. Moreover, normalization of this technology will only encourage more cameras and the buildup of an even more invasive surveillance architecture, upsetting the balance between individual rights and government intrusion.

These concerns are not merely theoretical. In other countries, we are already seeing face recognition being used as part of comprehensive surveillance systems that monitor and track citizens. For example, China has 200 million surveillance cameras and is working to develop the capability to identify any citizen within seconds.[xii] The government is amassing face recognition databases of individuals who have mental illnesses, used drugs, or petitioned the government with grievances. The government is also using the technology as a tool to track and suppress ethnic minorities, including the Uighur population. For example, China reportedly keeps a face recognition database of all Uighurs who leave the province of Xinjiang, and are developing systems that can alert police when a Uighur moves into a new neighborhood.[xiii] It is critical that we safeguard against the buildup of a similar surveillance architecture in the U.S., which would undermine our constitutional values.

II. Current uses of face recognition violate the Fourth Amendment

Many common uses of face recognition by law enforcement threaten core constitutional rights, including those under the Fourth Amendment. Specifically, use of face recognition that permits law enforcement to infer the location of an individual, deduce intimate details of a person's life,

or subject countless individuals to scrutiny based merely on the presence of their photo in a database raise particularly pronounced constitutional concerns.

Federal, state, and local law enforcement agencies have used face recognition hundreds of thousands of times. Yet, no Court of Appeals has issued an opinion involving real-time face recognition tracking or matching against large-scale databases, like a drivers' license repository. This is no accident. There are not many face recognition cases coming before courts in part because the government is not complying with its constitutional obligation to provide notice to criminal defendants, including in cases where face recognition could constitute exculpatory evidence under *Brady*.[xiv] For example, the Pinellas County Sheriff's Office in Florida has been using a face recognition system in its investigations since 2001, yet the county public defender has reportedly never received face recognition information as *Brady* evidence.[xv]

Though there are few cases that directly address the use of face recognition, the Supreme Court has repeatedly rejected "mechanical interpretation[s]" of the Fourth Amendment that would "permit police technology to erode the privacy guaranteed by the Fourth Amendment."[xvi] For example, in *Kyllo* the court rejected arguments that use of thermal imaging cameras to see inside a house did not require a warrant because the technology allowed the government to "explore details of the home that would previously have been unknowable without physical intrusion."[xvii] Similarly, in *Riley* the court declined to apply the search-incident-to-arrest exception to the warrant requirement to search of a cell phone, noting that cell phones differ in both "a quantitative and a qualitative sense" from the types of objects traditionally found on a person and can have "immense storage capacity."[xviii] And, in *Carpenter,* the court ruled that a warrant was required to obtain historical cell site location information, noting among other things that the "retrospective quality of the data" can "give police access to a category of information otherwise unknowable."[xix]

Similar to the technologies the Supreme Court confronted in *Kyllo*, *Riley,* and *Carpenter,* the use of face recognition permits law enforcement to obtain information about individuals that has traditionally been safeguarded from government intrusion. Face recognition can be used on photographs to determine who people associate with and where they have been. Combined with the increased number of cameras and available video footage, it can be used to reconstruct an individual's movements in a large area over a significant period of time. Developments in real-time capabilities may also soon allow police to identify someone nearly instantaneously by, for example, matching an image from a body worn camera against a database of millions of photos. Such uses can provide an "intimate window into a person's life," including whether they attend a protest, visit the doctor, or meet with a criminal defense attorney.

The fact that face recognition relies on a biometric characteristic – a person's face – means that it is virtually impossible for an individual to insulate themselves from this kind of surveillance. In this sense, face recognition is potentially even more invasive than some of the technologies the Supreme Court has previously examined. Nonetheless, in most cases, it is being used to gather the types of sensitive information referenced above without a warrant or judicial scrutiny of any kind, contrary to the guidance provided by *Carpenter* and other cases.

Moreover, developments in face recognition allow the government to obtain information cheaply and on a scale that would previously have been impossible, increasing the risk of abuse. Unlike eyewitness identifications, law enforcement can conduct thousands of searches matching against millions of photos – for less than the cost of a pizza.[xx] In many cases, they take advantage of large-scale databases, such as driver's license or passport repositories, that were never meant for routine investigative use. As a result, police effectively are able to conduct a search of millions of faces, with just a few clicks of a button. In other words, "this newfound tracking capacity runs against everyone," including individuals for whom there is no cause to believe committed a crime.[xxi] This ease, combined with the secretive nature of the technology, allows it to evade "the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[xxii]

III. The harms associated with face recognition will disproportionately fall on immigrant and communities of color

The dangers associated with law enforcement use of face recognition are likely to disproportionately impact immigrant and communities of color. This is for two main reasons. One, face recognition technology is disproportionally inaccurate on certain subgroups, including individuals with darker skin pigmentation. For example, a prominent study co-authored by an FBI expert found that leading facial recognition algorithms performed worse on African Americans and women.[xxiii] Higher rates of inaccuracy on darker skin pigmentations have also been noted in products marketed by private companies, including Amazon, Microsoft, and IBM.[xxiv] The effects of false identifications can be dire, leading to unjustified prosecutions and even false convictions.

Two, even if the technology was accurate, it is more likely to be used against communities of color, which are disproportionately subject to over policing, including increased stops, arrests, and uses of force. For example, African Americans are incarcerated at four times the rates of whites nationally.[xxv] In Maryland, African Americans are 29 percent of the state population but 68 percent of people in jails and prison; in Ohio, these numbers are 12 percent and 43 percent respectively.[xxvi] Moreover, in 2016, African Americans comprised 27 percent of all individuals arrested in the United States - double their share of the total population. Similarly, African Americans were 35 percent of juvenile arrests, but account for only 15 percent of the population.[xxvii] As a result of these disparities, African Americans and other vulnerable communities are also likely to be overrepresented in the mugshot photos that some facial recognition systems scan for potential matches.

While a warrant requirement can provide enhanced protection, studies have shown that this alone does not eliminate racial disparities. A study examining narcotics search warrants in the San Diego Judicial District found that African Americans and Hispanics were overrepresented as targets of such warrants relative to their population and patterns of drug use. The study found that 98 percent of the examined search warrants for cocaine targeted African American and Hispanic residents (potentially due to law enforcement's disproportionate focus on crack cocaine), and Hispanics were overrepresented as targets of methamphetamine warrants.[xxviii] Thus, use of face recognition, without safeguards to address existing policing abuses and disparities, risks further exacerbating such problems.

IV. Congress should press FBI, ICE, and other federal agencies to adopt a federal moratorium on face recognition for immigration and law enforcement purposes, particularly in light of these agencies' failure to adopt sufficient safeguards

When the FBI first began developing its biometric and face recognition capabilities, it assured Congress that it would take steps to protect individuals' rights. The agency has consistently broken those promises. Despite the FBI's continued efforts to expand the collection and use of biometrics, including face recognition, it has failed to take even basic steps to ensure that individuals' rights are not violated. Similarly, other federal agencies also appear to be using face recognition without appropriate safeguards.

The ACLU urges Congress to take action to prevent federal agencies, including the FBI, from using face recognition for criminal and immigration enforcement purposes until Congress fully debates and passes legislation dictating what, if any, uses are permissible. In addition, we urge the Committee to fully utilize its oversight powers to obtain and make public information regarding (1) in what circumstances are federal agencies, including the FBI and ICE, using or piloting face recognition; (2) whether agencies are complying with their constitutional notice obligations, including in cases where face recognition may be exculpatory evidence; (3) how federal agencies are implementing the *Carpenter* decision and applying it to face recognition, (4) whether face recognition products being deployed are accurate; and (5) what policies and procedures are in place to ensure that face recognition does not violate individuals' rights.

a. FBI use of face recognition

The FBI's Next Generation Identification (NGI) database, which was launched in 2008 and became fully operational in 2014, stores a host of biometric information, including iris scans, photos, and voice prints.[xxix] The database includes records of millions of Americans who have never been accused of a crime, such as those who have applied for a background check as a condition of employment, been arrested but never charged, or who have applied to become permanent residents or citizens. Through the NGI's Interstate Photo System (NGI-IPS), the FBI operates a face recognition system with over 30 million mugshots, which can be accessed by the FBI and various state and local law enforcement agencies.[xxx] The FBI is also reportedly piloting use of Amazon's face recognition product, "Rekognition", though the agency has not disclosed details of the pilot and how it may interact with NGI-IPS or other agency systems.[xxxi]

In addition to NGI-IPS, the FBI's Facial Analysis Comparison and Evaluation (FACE) services is able to search databases maintained by the Department of Defense, State Department (including U.S. citizen passport application photos), and the drivers' license database of at least 15 states.[xxxii] Collectively, there are over 411 million face photos available in all searchable repositories.[xxxiii] From August 2011 through December 2015, the FBI requested almost 215,000 searches of external partners' databases.[xxxiv]

Despite assurances to Congress, the FBI has failed to take the steps necessary to ensure the face recognition services it uses are accurate and contain sufficient safeguards to protect individuals'

rights. In a 2012 hearing before the Senate Judiciary Subcommittee on Privacy, Technology and the Law, the FBI committed to developing an audit system to prevent law enforcement agencies from using NGI-IPS for impermissible purposes, like identifying individuals at a protest. [xxxv] However, according to the Government Accountability Office (GAO), the agency has not fully complied with recommendations to develop and implement a comprehensive audits plan to measure whether the system is being used in a way that protects individuals' privacy.[xxxvi] In addition, the FBI has failed to assess how often errors occur using the NGI database, has assumed no responsibility to assess the accuracy of the database of its state and federal partners, and has failed to conduct timely privacy assessments of the NGI database, as required by law. [xxxvii]

States have also raised concerns with use of states driver's license repositories by federal agencies for face recognition. In 2017, Vermont suspended use of the driver's license database by the FBI and other law enforcement agencies over concerns that such use violated state law.[xxxviii] The decision followed reports that Vermont had conducted concerning face recognition searches on behalf of federal agencies, including a request from the U.S. Marshals for information about a fugitive's girlfriend absent allegation of criminal wrongdoing; a request from the FBI based on nothing more than an allegation that an individual asked "unusual and suspicious" questions at a gun shop; and several requests for information from ICE and DHS.[xxxix]

Given these deficiencies, the FBI should halt their use of face recognition. Instead, they have doubled down. The FBI has continued to work to expand its access to states' driver license photos, and has also exempted the NGI from requirements in the Privacy Act designed to ensure that Americans are able to correct their data or go to court in cases where they feel their rights are being violated.[xl] In addition, it is unclear what, if any, procedures the agency has in place to ensure it complies with its constitutional notice obligations.

b. Other federal agencies' use of face recognition

Other federal agencies similarly appear to be utilizing face recognition without appropriate safeguards. For example, ICE reportedly obtains face recognition capabilities through use of CBP and Department of State databases, but has not disclosed how many searches it conducts and for what purposes.[xli] CBP and TSA have also announced comprehensive plans to deploy face recognition at airports across the country, despite the fact that the agencies have not even engaged in rulemaking.[xlii] The U.S. Secret Service is conducting a face recognition pilot program, which will scan individuals passing by on public streets and in areas adjacent to the White House.[xliii]

Congress must intervene to halt the continued use of face recognition and other biometric technologies by the FBI and other federal agencies until individual rights can be appropriately safeguarded through legislation. We also urge the committee to utilize its oversight powers to make public more information about use of face recognition by FBI, ICE, and federal agencies of law enforcement and immigration enforcement purposes.

V. Congress should investigate private companies that sell face recognition to law enforcement without safeguards to prevent rights violations

A host of companies are aggressively marketing face recognition products for law enforcement purposes. Many of these companies boast that their products can be relied on for everything from identifying someone during a police encounter to reconstructing past movements from video footage. However, there is ample evidence that marketing face recognition for these uses is both reckless and irresponsible, jeopardizing the safety and rights of countless communities.

Additional Congressional oversight in this area is essential. The ACLU urges the Committee to investigate companies that sell face recognition for law enforcement use, including Amazon and Microsoft to assess (1) the accuracy and bias of their products; (2) whether their marketing inadvertently or deliberately obscures the risk of law enforcement use or likelihood of error; (3) who they are selling/marketing this technology to and for what purposes; and (4) whether they have adopted sufficient safeguards to prevent their technology from being used to violate individuals' rights.

a. Amazon's "Rekognition"

In recent months, there has been significant scrutiny of Amazon's face recognition product, "Rekognition" – yet the company has failed to fully respond to Congressional requests for information or take steps to prevent the harms posed by its product.[xliv] Amazon boasts that Rekognition can identify up to 100 faces in a single image, track people in real time through surveillance cameras, and scan footage from body worn cameras.[xlv] Documents obtained by the ACLU of Northern California demonstrate that Amazon has aggressively worked with police departments to push some of the most pernicious uses of the technology, suggesting that it be integrated into body worn cameras for real-time identification or used in public areas.[xlvi]

The Washington County Sheriff's Office in Hillsboro, Oregon has already reportedly started using Amazon Rekognition to compare people's faces against a mugshot database of over 300,000 photos, including in cases involving misdemeanors like alleged shoplifting less than fifteen dollars in goods.[xlvii] Similarly, the Orlando Police Department is reportedly piloting a version of Rekognition that would allow it to scan the footage from public cameras, including traffic cameras, ultimately permitting identification of "people of interest."[xlviii] In both Oregon and Orlando, Rekognition has been used absent any authorizing legislation, public debate, or independent auditing, or transparent policy.

The aggressive marketing of Rekognition is particularly concerning given public concern, independent testing questioning its accuracy, and the company's refusal to respond to Congressional requests for more information. In a test by the ACLU of Northern California comparing publicly available portrait photos of members of Congress against 25,000 mugshots, the product falsely matched 28 members, including Representatives Clay, Gomez, and DeSaulnier who sit on this Committee. Forty percent of the false matches were Members of color. To obtain the software, the ACLU of Northern California needed only an Amazon account, and $12.33 to run the tests.[xlix] Similarly, in a study by MIT Media lab, Rekognition misclassified women as men 19 percent of the time and mistook darker-skinned women for men

31 percent of the time.[l] Despite sharing the results with Amazon, seven months later a test of the software revealed the same rates of inaccuracy.[li]

Despite questions about both the accuracy and civil rights implications of Rekognition, Amazon has continued to bury its head in the sand. It has ignored the call of over 150,000 individuals, more than 85 organizations,[lii] shareholders,[liii] employees,[liv] and its former lead technology officer[lv] to stop selling the technology to government. Even more, it has shunned Congressional oversight efforts. Despite inquiries from over 60 members of Congress,[lvi] the company has refused to respond to several basic requests for information, including a list of law enforcement departments that currently use the technology and whether any of these departments have a history of discriminatory policing. Indeed, the company's response to inquiries demonstrates that it has no means of fully auditing use or otherwise ensuring that its technology is used consistent with the terms of service.[lvii] Thus, if an individual used the technology to, for example, identify children outside a school, the company would not have any means of knowing about such use or taking steps to prevent impacted children's privacy. Given the concerns with Rekognition, the lack of oversight over the technology and its widespread availability are even more disturbing.

b. Other Face Recognition Products

Amazon is not the only company that markets and sells face recognition technology. Microsoft also markets its technology for law enforcement uses. While the company has acknowledged that use of face recognition can threaten civil rights and should be subject to robust limits, it too has ignored the calls from over 85 groups[lviii] to stop selling this technology to the government and has not disclosed the standards that officials must meet to use their product.

Cognitec[lix], Idemia[lx] (includes what was formerly MorphoTrust USA), Gemalto[lxi] (which is now a part of the Thales Group), Vigilant Solutions[lxii] (recently acquired by Motorola), FaceFirst[lxiii], and other companies are also reportedly marketing face recognition products for government use. For example, FaceFirst markets its product for law enforcement to identify people in real-time during interactions, like a traffic stop,[lxiv] and its product is reportedly used by retailers to scan all customers who enter a store (without consent) to identify individuals who are alleged shoplifters.[lxv] Little public information is available regarding who currently uses these companies' technologies, how accurate their technologies are, or how they prevent their technology from violating individuals' rights.

The approach of these companies contrasts with Google, who has said it will not make a face recognition product available until the concerns with the technology can be addressed, which is an important first step.[lxvi] Similarly, Kairos, has said it will not sell its face recognition product to law enforcement[lxvii] and its former CEO has stated that he believes that use of face recognition "in law enforcement or in government surveillance of any kind is wrong — and that it opens the door for gross misconduct by the morally corrupt."[lxviii]

Given the flurry of industry activity in this area, Congressional oversight over this industry is essential. We urge this Committee to demand that Amazon fully respond to Congressional requests for information about their product. In addition, we urge the committee to obtain and

make public information regarding the face recognition products of other companies, including: which law enforcement departments use the products; what uses the products are being marketed and sold for; the accuracy and reliability of the products; and what protections are in place to prevent the products from violating individuals' rights.

VI. Conclusion

When it comes to face recognition, law enforcement agencies have put the cart before the horse. Federal, state, and local police continue to expand the use of this controversial technology - even amid ample evidence that it is not being used consistent with our core constitutional values. Congress should press federal agencies to hit the pause button and stop using this technology until rights can be safeguarded and there is a democratic process dictating what, if any, uses are appropriate. In addition, this Committee should use its vast oversight powers to hold companies that continue to market dangerous uses of face recognition accountable and to make public additional information about the extent that this technology is being deployed by federal agencies for immigration and law enforcement purposes.

---

[i] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country. With more than three million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico and Washington, D.C., to preserve American democracy and an open government.

[ii] Alle Manning, *A False Facial Recognition Match Cost This Man Everything*, Vocativ (May 1, 2017), https://www.vocativ.com/418052/false-facial-recognition-cost-denver-steve-talley-everything/index.html; Lance Hernandez, *Man arrested for bank robbery files $10 million suit against Denver Police Department*, The Denver Channel (Sept. 15, 2016), https://www.thedenverchannel.com/news/local-news/man-arrested-for-bank-robbery-files-10-million-suit-against-denver-police-department.

[iii] Russell Brandom, *Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protestors*, The Verge (Oct. 11, 2016) https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api. ("The ACLU's report includes direct evidence the tool was used to monitor unrest after the death of Freddie Gray in Baltimore, in the form of a testimonial provided by Geofeedia to an unnamed police department.")

[iv] Sameer Rao, *Maryland woman says she received death threats after Sri Lanka misidentified photo of her as a bombing suspect,* Baltimore Sun (Apr. 26, 2019), https://www.baltimoresun.com/news/maryland/baltimore-county/bs-md-amara-majeed-cair-20190426-story.html.

[v] Benjamin Conarck, *How an accused drug dealer revealed JSO's facial recognition network*, The Florida Times Union (Nov. 11, 2016), https://www.jacksonville.com/public-safety/2016-11-11/how-accused-drug-dealer-revealed-jso-s-facial-recognition-network.

[vi] S.F., Cal., Ordinance File No. 190110 (May 6, 2019) *available at* https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A.

[vii] S. 1385, 191st General Court, 1st Annual Sess. (Mass. 2019) *available at* https://malegislature.gov/Bills/191/S1385.

[viii] ACLU, *Community Control Over Police Surveillance,* https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance.

[ix] Letter from United States Securities and Exchange Commission to Ronald Mueller, (Apr. 3, 2019), *available at* https://cdn.vox-cdn.com/uploads/chorus_asset/file/16008565/SEC_Amazon.com__Inc._SEC_Response__2_.pdf.

[x] Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame, and Lots of Cameras*, NY Times (July 18, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[xi] *United States* v. *Jones*, 565 U.S. 400, 416 (Sotomayor, J., concurring) (quotations omitted).

[xii] *Id. See also* Jon Russell, *China's CCTV Surveillance Network Took Just 7 minutes to Identify a Reporter*, Tech Crunch, https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/
[xiii] Paul Mozur, *One-month, 500,000 Scans: How China is Using A.I. to Profile a Minority*, NY Times (April 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
[xiv] *Brady v. Maryland*, 83 S. Ct. 1194 (1963).
[xv] *See* Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up*, (Oct. 18, 2018), *available at* https://www.perpetuallineup.org.
[xvi] *Kyllo v. United States*, 533 U.S. 27, 28 (2001).
[xvii] *Kyllo*, 533 U.S. at 121.
[xviii] *Riley v. California*, 573 U.S. 373, 393 (2014).
[xix] *Carpenter v. United States.*, 138 S. Ct. 2206, 2218 (2018).
[xx] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots,* ACLU (July 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.
[xxi] *Carpenter*, 138 S. Ct. at 2218.
[xxii] *Jones*, 565 U.S. at 416 (2012) (Sotomayor, J., concurring) (citing Illinois v. Lidster, 540 U. S. 419, 426 (2004)).
[xxiii] Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, Vol. 7, IEEE Transactions On Information Forensics And Security, 1789 (Dec. 2012), *available at* https://assets.documentcloud.org/documents/2850196/Face-Recognition-Performance-Role-of-Demographic.pdf.
[xxiv] Tom Simonite, *Photo Algorithms ID White Men Fine - Black Women, Not So Much*, Wired (Feb. 6, 2018), https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much/.
[xxv] NAACP, *Criminal Justice Fact Sheet*, https://www.naacp.org/criminal-justice-fact-sheet/.
[xxvi] Prison Policy Initiative, *Ohio Profile*, https://www.prisonpolicy.org/profiles/OH.htmlcite; Prison Policy Initiative, *Maryland Profile*, https://www.prisonpolicy.org/profiles/MD.html.
[xxvii] Sentencing Project, Report to the United Nations on Racial Disparities in the U.S. Criminal Justice System (April 19, 2018), https://www.sentencingproject.org/publications/un-report-on-racial-disparities/.
[xxviii] Laurence A. Benner, *Racial Disparity in Narcotics Search Warrants*, 183, Gender Race & Just. (2002) *available at* https://heinonline.org/HOL/LandingPage?handle=hein.journals/jgrj6&div=13&id=&page=.
[xxix] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. 7 (2012); FBI Press Release, *FBI Announces Full Operational Capability of the Next Generation Identification System* (Sept. 15, 2014), https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational- capability-of-the-next-generation-identification-system.
[xxx] U.S. Gov't Accountability Office, GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI Should Better Ensure Privacy and Accuracy (May 2016), https://www.markey.senate.gov/imo/media/doc/Rekogntion%20Markey%20Response.pdf.
[xxxi] Frank Konkel, *The FBI is Trying Amazon's Facial-Recognition Software*, Netxtgov (Jan. 3, 2019), https://www.nextgov.com/emerging-tech/2019/01/fbi-trying-amazons-facial-recognition-software/153888/.
[xxxii] The following states have partnered with the FBI's Facial Analysis, Comparison, and Evaluation (FACE) Services Unit: Alabama, Arkansas, Delaware, Illinois, Iowa, Kentucky, Michigan, Nebraska, New Mexico, North Carolina, North Dakota, South Carolina, Tennessee, Texas, Utah, and Vermont. 2016 GAO Report, *supra note xxx,* at 51. Vermont issued a moratorium on face recognition use of its driver's license repository in 2017.
[xxxiii] *Id.* at 15.
[xxxiv] *Id.* at 17.
[xxxv] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. 7 (2012).
[xxxvi] Letter from U.S. Gov't Accountability Office to Att'y Gen. Barr, (Apr. 10, 2019), *available at* https://www.gao.gov/assets/700/698610.pdf.
[xxxvii] *Id.*
[xxxviii] Stewart Ledbetter, *Governor suspends Vermont DMV's facial recognition program*, NBC 5 (May 25, 2017), https://www.mynbc5.com/article/governor-suspends-vermont-dmvs-facial-recognition-program/9649084.
[xxxix] Letter from ACLU of Vermont to Robert Ide, (May 23, 2017), *available at* https://www.acluvt.org/sites/default/files/aclu-vt_letter_to_dmv_commissioner_ide_may_23_2017.pdf; Vermont

Dep't of Motor Vehicles, Agency of Transportation, Request for Facial Recognition Investigation, *available at* https://www.acluvt.org/sites/default/files/dmv_facial_recognition_program_search_requests_01-2013_-_04-2017_aclu_records_request_2016.pdf.

[xl] *See* DOJ, *Privacy Act of 1974; Implementation*, Federal Register Vol. 82 No. 146 (Aug. 1, 2016), *available at* https://www.govinfo.gov/content/pkg/FR-2017-08-01/pdf/2017-15423.pdf.

[xli] Letter from U.S. Immigrations and Customs Enforcement to Sen. Ron Wyden, (Oct. 16, 2018), *available at* https://www.pogo.org/document/2018/10/ice-response-to-sen-wyden-inquiry-about-facial-recognition-technology/.

[xlii] *See* U.S. Customs and Border Patrol, *Biometric Breakthrough: How CBP is Meeting its Mandate and Keeping America Safe*, https://www.cbp.gov/frontline/cbp-biometric-testing; U.S. Transportation Security Administration, *TSA Biometrics Roadmap*, https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

[xliii] DHS, Privacy Impact Assessment for the Face Recognition Pilot, DHS/USSS/PIA-024 (November 26, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-frp-november2018.pdf. *See also* Jay Stanley, *Secret Service Announces Test of Face Recognition System Around White House*, ACLU (Dec. 4, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/secret-service-announces-test-face-recognition.

[xliv] *See* Matt Cagle & Nicole Ozer, *Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology*, ACLU, May 22, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new.

[xlv] Amazon, https://web.archive.org/web/20180125054549im_/https:/d1.awsstatic.com/diagrams/product-page-diagrams/Rekognition_Video_01.26c777dcffca35de99cd605ab0489487422aa90a.png (archived 2018).

[xlvi] *Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology, supra* note xliv.

[xlvii] Drew Harwell, *Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?*, Wash. Post (Apr. 30, 2019), https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/?utm_term=.71f93d40b974.

Martin Kaste, *Orlando Police Testing Amazon's Real-Time Facial Recognition*, NPR (May 22, 2018), https://www.npr.org/2018/05/22/613115969/orlando-police-testing-amazons-real-time-facial-recognition.

[xlix] *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots, supra* note xx. *See* Joy Buolamwini and Inioluwi Deborah Raji, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products, http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf.*

[l] *See* Joy Buolamwini and Inioluwi Deborah Raji, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products, http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf.*

[li] Natasha Singer, *Amazon Is Pushing Facial Technology That a Study Says Could Be Biased*, N.Y. Times (Jan. 24, 2019), https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html; Letter from Joy Buolamwini to Jeffrey Bezos, (June 25, 2018), *available at* https://uploads.strikinglycdn.com/files/e286dfe0-763b-4433-9a4b-7ae610e2dba1/RekognitionGenderandSkinTypeDisparities-June25-Mr.%20Bezos.pdf.

[lii] Letter from nationwide coalition of racial justice, faith, and civil, human, and immigrants' rights coalition to Jeffrey Bezos and David Zapolsky, (Jan. 15, 2019), *available at* https://www.aclu.org/coalition-letter-amazon-urging-company-commit-not-release-face-surveillance-product; Letter from nationwide coalition to Jeffrey Bezos, (June 18, 2018), *available at* https://www.aclu.org/letter-nationwide-coalition-amazon-ceo-jeff-bezos-regarding-rekognition; Letter from nationwide coalition to Jeffrey Bezos, (May 22, 2018), https://www.aclunc.org/docs/20180522_AR_Coalition_Letter.pdf.

[liii] Letter from Amazon shareholders to Jeffrey Bezos, (June 15, 2018), *available at* https://www.aclu.org/letter/letter-shareholders-amazon-ceo-jeff-bezos-regarding-rekognition.

[liv] James Vincent, *Amazon employees protest sale of facial recognition software to police*, The Verge (June 22, 2018), https://www.theverge.com/2018/6/22/17492106/amazon-ice-facial-recognition-internal-letter-protest.

[lv] *On Recent Research Auditing Commercial Facial Analysis Technology*, Medium (Mar. 26, 2019), https://medium.com/@bu64dcjrytwitb8/on-recent-research-auditing-commercial-facial-analysis-technology-19148bda1832.

[lvi] Letter from Sen. Ed Markey et al. to Jeffrey Bezos, (Nov. 29, 2018), *available at* https://www.markey.senate.gov/imo/media/doc/Bicameral%20Amazon%20Recognition.pdf; Letter from Rep. Jimmy Gomez et al. to Jeffrey Bezos, (July 27, 2018), *available at* https://gomez.house.gov/uploadedfiles/07272018_amazon_rekognition_letter_final.pdf; Letter from Sen. Ed Markey

et al. to Jeffrey Bezos, (July 26, 2018), *available at* https://www.markey.senate.gov/imo/media/doc/Amazon%20Facial%20Recognition%20Tech.pdf; Letter from Reps. Keith Ellison and Emanuel Cleaver to Jeffrey Bezos, (May 25, 2018), *available at* https://assets.documentcloud.org/documents/4484636/Ellison-Cleaver-Letter-to-Jeff-Bezos.pdf; Letter from Congressional Black Caucus to Jeffrey Bezos, (May 24, 2018), *available at* https://cbc.house.gov/uploadedfiles/final_cbc_amazon_facial_recognition_letter.pdf.

[lvii] Amazon Response Letter to Senator Markey, (Aug, 20, 2018), *available at* https://www.markey.senate.gov/imo/media/doc/Rekogntion%20Markey%20Response.pdf

[lviii] Letter from racial justice, faith, and civil, human, and immigrants' rights groups to Satya Nadella and Brad Smith, (Jan. 15, 2019), *available at* https://www.aclu.org/coalition-letter-microsoft-requesting-company-commit-not-release-face-surveillance-product.

[lix] *See* Cognitec, *Law Enforcement*, https://www.cognitec.com/applications-law-enforcement.html.

[lx] *See* Idemia, *Public security & law enforcement,* https://www.idemia.com/public-security-law-enforcement.

[lxi] *See* Gemalto, *Gemalto Cogent Automated Biometric Identification System (CABIS)*, https://www.gemalto.com/govt/biometrics/biometric-software/automated-biometric-identification-system.

[lxii] *See* Vigilant Solutions, *Products*, https://www.vigilantsolutions.com/products/.

[lxiii] *See* FaceFirst, *Facial Recognition for Law Enforcement*, https://www.facefirst.com/industry/law-enforcement-face-recognition/.

[lxiv] *See* FaceFirst Facial Recognition Platform, *Mobile Face Recognition for Law Enforcement by FaceFirst*, Youtube (Oct. 6, 2017), https://www.youtube.com/watch?v=kuvr2nJnHwo.

[lxv] Leticia Miranda, *Thousands Of Stores Will Soon Use Facial Recognition, And They Won't Need Your Consent*, BuzzFeed (Aug. 17, 2018), https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at.

[lxvi] Kent Walker, *AI for Social Good in Asia Pacific,* Google (Dec. 13, 2018), https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/amp/.

[lxvii] Megan Rose Dickey, *Kairos gets a $4 million lifeline for its facial recognition software*, TechCrunch (Feb. 2019), https://techcrunch.com/2019/02/19/kairos-gets-a-4-million-lifeline-for-its-facial-recognition-software/.

[lxviii] Brian Brackeen, *Facial recognition software is not ready for use by law enforcement,* TechCrunch (June. 2018), https://techcrunch.com/2018/06/25/facial-recognition-software-is-not-ready-for-use-by-law-enforcement/.