Nicol Turner Lee and Caitlin Chin

Police surveillance and facial recognition: Why data privacy is imperative for communities of color

https://www.brookings.edu/ Tuesday April 12, 2022

Editor's Note:
This paper was originally presented at the American Bar Association's Antitrust Spring Meeting on April 8, 2022, in Washington, D.C.

INTRODUCTION

Governments and private companies have a long history of collecting data from civilians, often justifying the resulting loss of privacy in the name of national security, economic stability, or other societal benefits. But it is important to note that these trade-offs do not affect all individuals equally. In fact, surveillance and data collection have disproportionately affected communities of color under both

From the historical surveillance of civil rights leaders by the Federal Bureau of Investigation (FBI) to the current misuse of facial recognition technologies, surveillance patterns often reflect existing societal biases and build upon harmful and virtuous cycles. Facial recognition and other surveillance technologies also enable more precise discrimination, especially as law enforcement agencies continue to make misinformed, predictive decisions around arrest and detainment that disproportionately impact marginalized populations.

In this paper, we present the case for stronger federal privacy protections with proscriptive guardrails for the public and private sectors to mitigate the high risks that are associated with the development and procurement of surveillance technologies. We also discuss the role of federal agencies in addressing the purposes and uses of facial recognition and other monitoring tools under their jurisdiction, as well as increased training for state and local law enforcement agencies to prevent the unfair or inaccurate profiling of people of color. We conclude the paper with a series of proposals that lean either toward clear restrictions on the use of surveillance technologies in certain contexts, or greater accountability and oversight mechanisms, including audits, policy interventions, and more inclusive technical designs.

THE HISTORY OF RACE AND SURVEILLANCE IN THE UNITED STATES

The oversurveillance of communities of color dates back decades to the civil rights movement and beyond. During the 1950s and 1960s, the FBI tracked Martin Luther King, Jr., Malcolm X, and other civil rights activists through its Racial Matters and COINTELPRO programs, without clear guardrails to prevent the agency from collecting intimate details about home life and relationships that were unrelated to law enforcement.[1] More recently, the Black Lives Matter (BLM) movement, initially sparked in 2013 after the murder of 17-year-old Trayvon Martin by a local vigilante, has highlighted racial biases in policing that disproportionately lead to unwarranted deaths, improper arrests, and the excessive use of force against Black individuals.[2] Over the years, the government's response to public protests over egregious policing patterns has raised various concerns over the appropriate use of surveillance, especially when primarily focused on communities of color. In 2015, the Baltimore Police Department reportedly used aerial surveillance, location tracking, and facial recognition to identify individuals who publicly protested the death of Freddie Gray.[3] Similarly, after George Floyd was murdered in 2020, the U.S. Department of Homeland Security (DHS) deployed drones and helicopters to survey the subsequent protests in at least 15 cities.[4]

But African Americans are not the only population that has been subjected to overt tracking and profiling. The consequences of mass government surveillance were evident in programs like the China Initiative, which the Department of Justice (DOJ) launched in 2018 to prevent espionage and intellectual property theft and formally ceased in February 2022.[5]

Although the China Initiative aimed to address national security threats from the Chinese government, it manufactured wider distrust and racial profiling of Chinese American academics, including those who were U.S. citizens or who lacked ties with the Chinese Communist Party. It led to several false arrests, including those of Temple University professor Xi Xiaoxing, UCLA graduate student Guan Lei, University of Tennessee professor Anming Hu, and National Weather Service scientist Sherry Chen.[6] Like with other historically-disadvantaged populations, government surveillance of Asian Americans is not a new phenomenon. As an example, the U.S. government monitored the broader Japanese American community for years even prior to World War II, including by accessing private communications and bank accounts, and eventually used census data after 1941 to locate and detain 120,000 people in internment camps.[7]

Demonstrating similar profiling of an entire community, the New York Police Department (NYPD) and Central Intelligence Agency (CIA) surveilled Muslim neighborhoods, restaurants, mosques, stores, and student groups for over six years after September 11, 2001, listening in on conversations, recording license plates, and taking videos.[8] Over a decade after 9/11, a 2017 Pew Research Center survey found that 18% of Muslim American respondents still experienced being "singled out by airport security."[9] From 2015 to 2020, Freedom of Information Act (FOIA)

records exposed over 75 complaints sparked by intrusive airport searches or Islamophobic comments from Transportation Security Administration (TSA) officers toward people who were perceived to be of Middle Eastern descent.[10] Both the NYPD's "Demographic Unit" surveillance and TSA's profiling of Muslim travelers are widely considered to be inaccurate and ineffective in preventing violent crime.[11]

Moreover, Customs and Border Protection (CBP) has deployed planes, boats, and radios to track and identify people along the U.S.-Mexico border—continuing a long tradition of hostility toward immigrants, especially those from Latino communities. Immigrant-focused surveillance extends far beyond a physical border; during the Obama and Trump administrations, Immigration and Customs Enforcement (ICE) purchased surveillance technology from private companies like Palantir and Thomson Reuters and used vehicle, insurance, tax, social media, and phone records to track undocumented immigrants throughout the country.[12] As early as 1992, the Drug Enforcement Administration surveilled phone call records to over 100 countries in bulk, which, over the years, may have gathered a significant amount of information from immigrants who called home to Mexico and countries in Central or South America.[13]

In these and other cases, government entities directed surveillance with the stated goals of maintaining public order, preventing cyber theft, and protecting Americans more broadly—but the indiscriminate deployment and public vigilantism have contributed to and been fueled by deep-rooted discrimination that affects communities of color in the United States. In order to stop ongoing injustice, we need greater attention to this issue and concrete steps to protect personal privacy.

HOW LAW ENFORCEMENT OFFICERS USE FACIAL RECOGNITION AND OTHER SURVEILLANCE TECHNOLOGIES

Although suspicion toward communities of color has historical roots that span decades, new developments like facial recognition technologies (FRT) and machine learning algorithms have drastically enlarged the precision and scope of potential surveillance.[14] Federal, state, and local law enforcement agencies often rely upon tools developed within the private sector, and, in certain cases, can access massive amounts of data either stored on private cloud servers or hardware (e.g., smartphones or hard drives) or available in public places like social media or online forums.[15] In particular, several government agencies have purchased access to precise geolocation history from data aggregators that compile information from smartphone apps or wearable devices. In the general absence of stronger privacy protections at the federal or state levels to account for such advancements in technology, enhanced forms of surveillance used by police officers pose significant risks to civilians already targeted in the criminal justice system and further the historical biases affecting communities of color. Next, we present tangible examples of how the private and public sectors both play a critical role in amplifying the

reach of law enforcement through facial recognition and other surveillance technologies.

(A) Facial recognition

Facial recognition has become a commonplace tool for law enforcement officers at both the federal and municipal levels. Out of the approximately 42 federal agencies that employ law enforcement officers, the Government Accountability Office (GAO) discovered in 2021 that about 20, or half, used facial recognition. In 2016, Georgetown Law researchers estimated that approximately one out of four state and local law enforcement agencies had access to the technology.[16]

On the procurement side, Clearview AI is one of the more prominent commercial providers of FRT to law enforcement agencies. Since 2017, it has scraped billions of publicly available images from websites like YouTube and Facebook, and enables customers to upload photos of individuals and automatically match them with other images and sources in the database.[17] As of 2021, the private startup had partnered with over 3,100 federal and local law enforcement agencies to identify people outside the scope of government databases. To put this tracking in perspective, the FBI only has about 640 million photos in its databases, compared to Clearview AI's approximately 10 billion.[18]

But Clearview AI is only one of numerous private companies that U.S. government agencies partner with to collect and process personal information.[19] Another example is Vigilant Solutions, which captures image and location information of license plates from billions of cars parked outside homes, stores, and office buildings, and which had sold access to its databases to approximately 3,000 local law enforcement agencies as of 2016.[20] Vigilant also markets various facial recognition products like FaceSearch to federal, state, and local law enforcement agencies; its customer base includes the DOJ and DHS, among others.[21] A third company, ODIN Intelligence, partners with police departments and local government agencies to maintain a database of individuals experiencing homelessness, using facial recognition to identify them and search for sensitive personal information such as age, arrest history, temporary housing history, and known associates.[22]

In response to privacy and ethical concerns, and after the protests over George Floyd's murder in 2020, some technology companies, including Amazon, Microsoft, and IBM, pledged to either temporarily or permanently stop selling facial recognition technologies to law enforcement agencies.[23] But voluntary and highly selective corporate moratoriums are insufficient to protect privacy, since they do not stop government agencies from procuring facial recognition software from other private companies. Moreover, a number of prominent companies have noticeably not taken this pledge or continue to either enable or allow scaping of their photos for third-party use in facial recognition databases. Furthermore, government agencies can still access industry-held data with varying degrees of due process—for example, although they would require a warrant with probable cause to compel precise geolocation data from first-party service providers in many cases, they might be able to access a person's movement history without probable cause through other means, including by purchasing it from a data broker.[24]

(B) Data aggregators and private sector information

The enormous scale of information that the private sector collects can feed into broader law enforcement efforts, since federal, state, and local government agencies have multiple channels by which to access corporate data. From January to June 2020 alone, federal, state, and local law enforcement agencies issued over 112,000 legal requests for data to Apple, Google, Facebook, and Microsoft—three times the number of requests than they submitted five years prior—of which approximately 85% were accommodated, including some subpoenas or court orders that did not require probable cause.[25] In 2020, reports surfaced that federal law enforcement agencies like the FBI, ICE, CBP, Drug Enforcement Agency, and the U.S. Special Operations Command purchased smartphone app geolocation data—without a warrant or binding court order—from analytics companies like Venntel, X-Mode, and Babel Street.[26] ICE and CBP used this data to enable potential deportations or arrests, which demonstrates how geolocation can have singular consequences for immigrant communities, especially among populations of color.[27]

Although geolocation tracking is almost ubiquitous among smartphone apps, it also poses unique potential for harm—both since it enables the physical pursuit of an individual and because it allows entities to deduce extraneous details like sexual orientation, religion, health, or personal relationships from their whereabouts.

Law enforcement has also worked with commercial data aggregators to scan social media websites for photos and posts. In 2018, ICE used photos and status updates posted on Facebook to locate and arrest an immigrant using the pseudonym "Sid" in California—only one of thousands of individuals whom the agency reportedly tracks at any given point, aided by private data miners such as Giant Oak and Palantir.[28] On a local level, the Los Angeles Police Department reportedly pilot tested ABTShield, an algorithm developed by a Polish company, to scan millions of tweets from October to November 2020 for terms that included "protest,"

"solidarity," and "lives matter," despite concerns that such bulk surveillance could pose privacy harms to BLM activists without presenting a clear benefit to public safety.[29]

(C) Public-oriented and civilian surveillance

Technological advances have expanded government surveillance in traditionally "public" places, prompting legal questions over the boundaries between permissible or non-permissible data collection. For instance, the Electronic Frontier Foundation and University of Nevada estimate that over 1,000 local police departments fly drones over their communities.[30] The Chula Vista Police Department had dispatched drones for over 5,000 civilian calls as of March 2021, capturing images of individuals within public areas like sidewalks and parking lots.[31] Body-worn cameras, another common police resource, can function as an accountability safeguard in part as a response to BLM activism but also pose privacy concerns—particularly when videos of civilians in sensitive scenarios are retained for lengthy periods, used for facial recognition purposes, or even publicly posted online, or when bystanders in public areas are incidentally caught on camera.[32]

Lastly, the everyday use of store-bought devices or apps by residents complicates the curtailment of excessive surveillance. Private sector apps, such as Neighbors (an Amazon subsidiary, and integrated with Amazon's Ring video doorbell), NextDoor, and Citizen allow people to livestream, watch, and exchange opinions about potential crimes with other users in real-time, generating concerns over unconscious bias and privacy.[33] Surveillance cameras are becoming increasingly prevalent within private homes, restaurants, entertainment venues, and stores; hundreds of millions are estimated to operate smart security devices worldwide, some of which—such as Google Nest's Doorbell and the Arlo Essential Wired Video Doorbell—include built-in facial recognition capabilities.[34] Simultaneously, Amazon's Ring has partnered with almost 2,000 local law enforcement agencies to facilitate a process for officers to ask Ring users to voluntarily turn over their video recordings without the explicit use of a warrant.[35]

FACIAL RECOGNITION IS PERHAPS THE MOST DAUNTING OF THEM ALL

Mass surveillance affects all Americans through a wide suite of technologies—but facial recognition, which has become one of the most critical and commonly-used technologies, poses special risks of disparate impact for historically marginalized communities. In December 2020, the New York Times reported that Nijeer Parks, Robert Williams, and Michael Oliver—all Black men—were wrongfully arrested due to erroneous matches by facial recognition programs.[36] Recent studies demonstrate that these technical inaccuracies are systemic: in February 2018, MIT and then-Microsoft researchers Joy Buolamwini and Timnit Gebru published an analysis of three commercial algorithms developed by Microsoft, Face++, and IBM, finding that images of women with darker skin had misclassification rates of 20.8%-34.7%, compared to error rates of 0.0%-0.8% for men with lighter

skin.[37] Buolamwini and Gebru also discovered bias in training datasets: 53.6%, 79.6%, and 86.2% of the images in the Adience, IJB-A, and PBB datasets respectively contained lighter-skinned individuals. In December 2019, the National Institute of Standards and Technology (NIST) published a study of 189 commercial facial recognition programs, finding that algorithms developed in the United States were significantly more likely to return false positives or negatives for Black, Asian, and Native American individuals compared to white individuals.[38] When disparate accuracy rates in facial recognition technology intersect with the effects of bias in certain policing practices, Black and other people of color are at greater risk of misidentification for a crime that they have no affiliation with.

Some companies have publicly announced unilateral actions to improve the accuracy of their facial recognition algorithms and diversity of their training datasets—but the scope and effectiveness of such efforts fluctuate across the enormous quantity and breadth of facial recognition vendors.[39] The question of accuracy is magnified when factoring in the general lack of transparency across the industry; companies are not legally required to allow third-party audits of their algorithms, and many either do not or selectively publish their processes and results. For example, Amazon chose not to submit its Rekognition algorithm for testing in NIST's 2018 report—even though, at the time, it was still licensing the algorithm for use by law enforcement agencies and in other highly-sensitive contexts.[40] Clearview AI has not publicly disclosed its rates of false positives or negatives, and similarly has not voluntarily submitted its algorithm for testing by NIST or another third party.[41]

Adding to the problem of errors in private sector facial recognition software, law enforcement databases are generally established with faulty data collection practices. Since historically biased policing patterns have contributed to their higher rates of interrogation and arrest, communities of color are often overrepresented in law enforcement databases compared to the overall U.S. population.[42] The National Association for the Advancement of Colored People (NAACP) reports that Black individuals are five times more likely than white individuals to be stopped by police officers in the United States, and that Black and Latino individuals comprise 56% of the U.S. incarcerated population but only 32% of the overall U.S. population.[43] This means that not only are police officers more likely to employ surveillance or facial recognition programs to compare images of Black and Latino individuals, but that mugshot images or arrest records of Black and Latino individuals are more likely to be stored in these databases in the first place—two distinct problems that, when aligned, will exacerbate existing patterns of racial inequity in policing.[44]

Apart from the dual challenges of accuracy and transparency, there remains an ethical question of if or when it is appropriate to use facial recognition to address legitimate security concerns, regardless of its accuracy. Even if facial recognition hypothetically could improve to a point where the technology itself has near-perfect accuracy rates across all demographic groups, it would still be possible for law enforcement officers to apply it in ways that replicate existing racial disparities

in their outcomes. When the European Parliament voted in favor of a non-binding resolution last October to prevent the mass police use of facial recognition in public places within the European Union (EU), it acknowledged this dilemma: "AI applications may offer great opportunities in the field of law enforcement…thereby contributing to the safety and security of EU citizens, while at the same time they may entail significant risks for the fundamental rights of people."[45]
Even if not fully banned from use in criminal justice, the institution of guardrails is a positive step toward more equitable use of enhanced surveillance technologies, including facial recognition. Any guardrails will need to consider the contexts in which technology is appropriate, such as with the European Commission's draft Artificial Intelligence Act that would restrict law enforcement's use of "real-time" facial recognition surveillance in public places to more "serious" situations like threats to physical safety, missing victims, or certain "criminal" offenses, and would direct law enforcement officers to take into account the nature and potential consequences of the crime before using facial recognition within the EU.[46] Weighing the need for both privacy and public safety, we now examine the existing legal guardrails that govern surveillance in law enforcement—and where gaps in privacy protections still remain.

THE APPLICATION OF EXISTING PRIVACY AND SURVEILLANCE SAFEGUARDS IN THE CONTEXT OF LAW ENFORCEMENT

The U.S. government has long acknowledged that surveillance cannot be unlimited. There must be some safeguards to prevent any privacy abuses by the government or private entities, as a matter of fundamental rights. To that end, federal, state, and local governments have enshrined privacy values into law—in certain contexts—through layers of constitutional principles, limited statutes, and court cases. However, new technology significantly shifts the traditional balance between surveillance and civil liberties, and the existing patchwork of laws may not be enough to prevent the risks stemming from facial recognition and other technologies.[47] As such, it is necessary to take stock of existing privacy safeguards and identify areas of improvement. Samuel Warren and Louis Brandeis described this phenomenon in their famous 1890 Harvard Law Review article: "That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."[48]

(A) How the law addresses government surveillance

In the United States, privacy principles can trace their roots to the Constitution.[49] Although the Fourth Amendment prevents the government from conducting "unreasonable" searches without probable cause to obtain a warrant, law enforcement officers can still collect data through other means, such as by purchasing personal information from data brokers or collecting data in public places where people do not possess a "reasonable expectation of privacy."[50] Yet, even the Supreme Court has acknowledged, in certain cases, that the amplifying

effect of technology in surveillance may require an examination of Fourth Amendment limitations in public places.[51] Although police officers can physically search people's vehicles subject to an arrest, the Court ruled in Riley v. California (2014) that they cannot search a person's smartphone without a warrant—acknowledging that smartphones are "a pervasive and insistent part of daily life … unheard of ten years ago" and the modern scope of data collection "calls for a new balancing of law enforcement and privacy interests."[52] Citing Riley, the Court held in Carpenter v. United States (2018) that the government would also require a warrant to compel cell phone service providers to turn over geolocation records, arguing that "seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's."[53]

Despite the majority opinions in Riley and Carpenter, there are limitations to the Supreme Court's ability to preserve privacy principles through judicial interpretation alone. In his dissent in Carpenter, then-Justice Anthony Kennedy wrote that the government's access of cell phone location records does not constitute a search under the Fourth Amendment, and individuals do not have a reasonable expectation of privacy in records controlled by a cell phone company. In another case, Florida v. Riley (1989), the Supreme Court held that police officers could fly a helicopter 400 feet above a greenhouse without a search warrant—even if the interior of the building would not be visible without aerial surveillance—and that people do not have a reasonable expectation of privacy if other helicopters could legally fly at that height and observe the activity from a public airspace.[54]

While the Supreme Court has heard several major cases on geolocation technologies, there is still legal and social uncertainty around surveillance technologies like facial recognition and drones, where judicial history is extremely limited, especially at the highest court.[55] One of the earliest court cases on facial recognition occurred in Lynch v. State (2018), when the First District Court of Appeal in Florida decided that a Black man named Willie Allen Lynch, who was identified by police through a facial recognition program, was not legally entitled to view the other four erroneous matches that the program returned.[56] The Michigan Court of Appeals recently decided one of the few cases related to drones, Long Lake Township v. Todd Maxon (2021), where it reversed a lower court's decision to rule that the government would require a warrant to surveil an individual's property with a drone.[57] In short, the judicial branch alone cannot manufacture privacy expectations—courts interpret existing law based on the Constitution, statutes, and regulations, but their interpretations depend on the judges or justices that sit on the bench, and it falls on Congress to resolve uncertainties.

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA), bundling the Wiretap Act and Stored Communications Act, to protect Americans against government privacy intrusions in their electronic communications (e.g., stored emails or live telephone conversations). However, the ECPA contains provisions that allow law enforcement to access emails and customer records without a warrant in certain contexts.[58] For example, law enforcement would require a warrant to access an unopened email that has been remotely stored for under 180 days—but after 180 days, it would be able to access that same email

with only a subpoena. It can also issue a subpoena to compel companies to turn over non-content user records such as name, address, and payment information. Apart from the ECPA, Executive Order 12333 and Section 702 of the Foreign Intelligence Surveillance Act allow the federal government to gather "incidental collection" of communications content from U.S. residents who contact people located outside the United States without a warrant, contrary to Fourth Amendment protections.[59] Together, these statutes and EO grant the U.S. government broad authority to access the electronic communications of Americans, tapping into the massive troves of data that private communications companies store.

Although facial recognition meets few enacted legal restrictions at the federal level, over seven states and 20 municipalities, such as Boston, San Francisco, and Virginia, have established some limitations on government use of facial recognition usage in certain contexts.[60] For instance, Maine enacted a law in 2021 that generally prohibits government use of facial recognition except in certain cases (e.g., "serious" crimes, identification of missing or deceased individuals, and fraud prevention).[61] The same year, Minneapolis passed an ordinance to prevent the government from procuring facial recognition technology from third parties (e.g., Clearview AI) or knowingly using information collected through facial recognition, citing the technology's higher misidentification rates for communities of color and the disproportionate burden of policing that communities of color face.[62] Yet, state and local regulations lack uniformity throughout the country, and the majority of municipalities do not have specific legal restrictions on government use of facial recognition.

(B) Protections from private companies

As we describe earlier, the private sector is integral to law enforcement operations; companies like Clearview AI often test and develop the facial recognition tools that are available to law enforcement or amass large databases that the government may have access to. Yet, in the absence of a nationwide comprehensive data privacy law, many companies face few legal limitations on how they collect, process, and transfer personal information—allowing Clearview and other companies to gather data from millions of people without clear controls to access or delete their images, and with few safeguards for security, algorithmic bias, and transparency.[63]

The Federal Trade Commission (FTC) primarily investigates and enforces data protection on a national level, relying on its authority under Section 5 of the FTC Act to act against entities that engage in "unfair or deceptive acts or practices." Using this authority, the FTC has entered consent agreements with companies like Sears (2009), Facebook (2011), Snapchat (2014), and Nomi Technologies (2015) for misrepresenting their privacy policies to their users.[64] However, this statute largely emphasizes user transparency, which has led to a system of "notice and choice," where companies display a lengthy privacy policy and require users to consent to it before accessing their service. Notice-and-choice does not effectively preserve privacy; companies like Clearview or Amazon's Ring can still set their own privacy policies—choosing what data they collect, store, and share, and for how

long—and with the FTC's more limited authority, the agency has only brought approximately 80 data privacy cases since 2002.[65]

Privacy regulations are disjointed at the state level, and only California, Colorado, and Virginia have so far enacted comprehensive data privacy laws that give residents the rights to access and delete personal information that many companies store. In addition, five states—Arkansas, California, Illinois, Texas, and Washington—have adopted laws that regulate how private companies treat biometric information, including facial recognition.[66] Companies have treated compliance with diverging state privacy laws in two primary ways: some, like Microsoft, have pledged to voluntarily offer single-state protections (e.g., the right to access personal information) nationwide, while others, such as Clearview AI, offer different privacy settings depending on where a person lives.[67] Clearview's website currently only allows California residents to access and delete their personal information, while Illinois residents may choose to opt out of search results.[68] Residents of the other 48 states do not experience these same privacy protections; they may submit a request for Clearview to remove search results associated with URLs that were already deleted from other websites but may not delete photos or opt out of search results for links that are still available elsewhere on the internet. Since Clearview does not advertise these controls, however, it is unclear how many individuals are aware of them or have submitted a data request. Despite its limited privacy controls, Clearview—along with many other facial recognition companies—does not ask individuals for permission to scrape their images from public places (e.g., CCTV surveillance cameras, social media platforms, other websites). This problem is widespread; a 2020 GAO report describes a study of 30 datasets used to train facial recognition algorithms since 2006, which revealed that approximately 24 million photos had been scraped from websites without obtaining consent from the one million individuals photographed.[69]

In the end, it is virtually impossible for an individual to fully opt out of facial recognition identification or control the use of their images without abstaining from public areas, the internet, or society altogether.

Since voluntary privacy protections do not apply across the entire industry—some companies offer privacy settings, while others do not—government intervention is

necessary to set privacy protections for all U.S. residents, especially those communities most vulnerable to the harmful effects of surveillance.

PROPOSALS TO PREVENT PRIVACY RISKS OF FACIAL RECOGNITION AND OTHER TECHNOLOGIES

As both the government and private corporations feed into the problem of surveillance, gaps in current federal and state privacy laws mean that their actions to collect, use, or share data often go unchallenged. In other words, existing laws do not adequately protect user privacy among the rising ubiquity of facial recognition and other emerging technologies, fundamentally omitting the needs of communities of color that disproportionately bear the consequences of surveillance. To reduce the potential for emerging technologies to replicate historical biases in law enforcement, we summarize recent proposals that address racial bias and unequal applications of technology in the public sector. We also explain why U.S. federal privacy legislation is necessary to govern how private sector companies implement fairness in the technical development process, limit their data collection and third-party sharing, and grant more agency to the individuals they surveil.

(A) Direct measures for federal, state, and local law enforcement agencies

Although the executive branch is taking some steps to evaluate its use of artificial intelligence and equitable distribution of public services, it lacks heightened federal government-wide scrutiny over its facial recognition programs and relationships with geolocation data brokers. In October 2021, the White House announced plans to develop an AI Bill of Rights to assert basic principles of civil liberties in technology, referencing the role that facial recognition plays in discriminatory arrests as well as the privacy concerns stemming from data collection.[70] In January 2021, the Biden administration issued an executive order that directed federal agencies to conduct equity assessments to review any obstacles that marginalized communities, including individuals of color, encounter to access government services and resources.[71] These are important steps, but the role of equity assessments should be extended to appraise the appropriateness of facial recognition, access to geolocation information from data brokers, and related privacy or civil rights implications for marginalized communities for the approximately 42 federal agencies that employ law enforcement officers in some function. Short of White House guidance, federal agency review of facial recognition technologies might remain more piecemeal; for example, the Internal Revenue Service announced in early February 2022 that it would stop using the facial recognition tool ID.me for citizen verification following public outcry, but it is unclear whether other federal agencies that use the software—such as the United States Patent and Trademark Office and Social Security Administration—will choose to do so as well.[72]

Federal law enforcement reform could also occur through an act of Congress, and legislators have introduced several bills that also propose new guardrails for executive agencies that conduct surveillance. In March 2021, the House of Representatives passed the George Floyd Justice in Policing Act which, among other provisions, would prohibit federal law enforcement officers from deploying facial recognition in their body cameras or patrol vehicle cameras.[73] The Facial Recognition and Biometric Technology Moratorium Act, which Sen. Ed Markey (D-Mass.) and Rep. Pramila Jayapal (D-Wash.) introduced in June 2021, aims to ban the federal government's use of biometric surveillance systems unless otherwise authorized by law.[74] The Facial Recognition Technology Warrant Act, which Sens. Chris Coons (D-Del.) and Mike Lee (R-Utah) proposed in 2019 during the previous Congress, included a warrant requirement for federal law enforcement officers to conduct "ongoing" surveillance of an individual in public areas with facial recognition for over 72 hours.[75] In April 2021, Rep. Jerrold Nadler (D-N.Y.) and Sen. Ron Wyden (D-Ore.) introduced The Fourth Amendment Is Not For Sale Act to mitigate federal law enforcement's access to information from "electronic communication services" or "remote computing services" in a way that violates privacy policy agreements or is otherwise deceptive, primarily targeting concerns over the government's purchase of geolocation information from data brokers like Venntel or X-Mode without a warrant.[76]

These proposed bills outline some of the existing problems with surveillance oversight: a lack of guardrails and transparency to prevent law enforcement's abuse of facial recognition and access to geolocation and communications data. Yet, they are not complete fixes. If enacted into law, the Fourth Amendment Is Not For Sale Act could prevent any attempts by law enforcement agencies to bypass due process or a probable cause warrant by purchasing communications or location data from private companies—but such a moratorium would be largely conditional on a website's terms of service or privacy policies.[77] Similarly, the George Floyd Justice in Policing Act, Facial Recognition Technology Warrant Act, and Facial Recognition Biometric Technology Moratorium Act could address federal law enforcement agencies' use of facial recognition, but would not affect state and local police officers' use of the technology.[78]

Because state and local governments have jurisdiction over policing in their areas, Congress and the federal executive branch have limited means to improve policing practices everywhere in the United States.[79] Still, as privacy concerns over facial recognition and surveillance grow, more state and local governments and police departments can individually consider measures to specify the contexts in which it is appropriate to use facial recognition and the necessary processes to do so (e.g., with a probable cause warrant).[80] In 2016, Georgetown Law researchers Clare Garvie, Alvaro Bedoya, and Jonathan Frankle proposed one possible framework for "acceptable uses of facial recognition" for law enforcement; for example, an individual with special training in facial recognition would be permitted to use the software to identify somebody on surveillance camera footage if officers have a "reasonable suspicion" that they committed a felony.[81] In addition to how to use the technology, such training would promote awareness of the "limitations of facial

recognition" and the "appropriateness [of images] for face recognition searches."[82] Ideally, this should also include an educational foundation in racial bias and ethics of surveillance for law enforcement officers at the federal, state, and local levels.

Brookings researcher Rashawn Ray has also supported training opportunities for state and local law enforcement as part of a holistic approach to increase accountability around racial profiling. Ray recently testified on this issue before the Virginia Advisory Committee to the U.S. Commission on Civil Rights, describing how police departments can host implicit bias and mental health trainings for officers, invite community members to sit on police oversight or misconduct trial boards, and provide housing stipends to help officers reside in their local communities.[83] Georgetown Law professor Laura Moy has also put forward a comprehensive list of questions that police departments might use to assess their use of surveillance technology, modeled after the racial equity impact assessments used by the Minneapolis Board of Education and others.[84] The proposals by Garvie, Bedoya, Frankle, Ray, and Moy are a valuable starting point for federal, state, and local law enforcement agencies to consider in application—and moreover, they demonstrate a need for police departments to actively work with civil society, academic researchers, and advocacy groups to provide input on prioritizing racial equity in police technology.

(B) The role of federal privacy legislation

Although Congress does not oversee state and local police departments, there is one clear-cut action it could take that would have an indirect—yet significant—impact on government surveillance across the nation: to pass a comprehensive federal privacy law that regulates the data practices of private companies. Government agencies often purchase or license facial recognition software from private companies, and businesses can either voluntarily share or be legally compelled to disclose large amounts of personal information to law enforcement.[85] Despite the general lack of comprehensive privacy regulations in the United States, the U.S. private sector provides unprecedented resources that immensely enhance the surveillance capabilities of law enforcement agencies.[86] Should Congress pass a federal privacy law to govern how private companies collect and use data, the effects would not only increase privacy protections for all Americans but reduce the possibility of surveillance abuse against communities of color in the law enforcement context.

First, Congress could introduce a requirement for businesses to allow individuals to access and delete personal information that they hold—allowing anybody to become aware of and erase their images in facial recognition databases like Clearview, and meaningfully increasing the transparency of data collection.[87] Next, Congress could enshrine common sense limitations in data collection, storage, and retention for private companies into law—this, in turn, would limit the amount of data that law enforcement agencies could access either voluntarily or through subpoenas or warrants. It should establish baseline principles like data

minimization—only allowing private companies to collect, use, and share data in ways that are necessary to the original business purpose—to reduce extraneous data collection and potential for surveillance. These principles are not inconceivable in practice: residents of California, Virginia, Colorado, and the European Union already possess similar protections, and pending legislation such as Sen. Maria Cantwell's (D-Wash.) Consumer Online Privacy Rights Act and Sen. Roger Wicker's (R-Miss.) SAFE DATA Act have been introduced to accord these provisions to all Americans.[88]

But Congress needs to go further than general privacy provisions and embody additional measures to address facial recognition and biometric information, given their outsized potential to result in disparate impact in the law enforcement context. Federal privacy legislation could also advance this objective; Congress could direct the Federal Trade Commission to study the impact of biometric information, including algorithmic outcomes, on civil rights in highly sensitive scenarios such as law enforcement. Current federal privacy bills or proposals take different approaches to biometric information—some, such as Sen. Sherrod Brown's (D-Ohio) draft Data Accountability and Transparency Act of 2021, would ban "data aggregators" from using facial recognition technology altogether, while on the other end of the spectrum, Wicker's SAFE DATA Act would simply require companies to obtain consent from individuals before processing or sharing biometric information with third parties.[89] Likely, some solution would be necessary in the middle: clear guardrails on how private companies collect, process, and transfer biometric information in a manner that would allow them to use and improve the technology in appropriate contexts while also preventing misuse. Congress could direct the FTC to create these regulations, based on the findings of their study and input from civil society.

Legislation can require businesses that use personal information to develop or deploy algorithms to audit both their products and outcomes to prevent disparate impact. A number of researchers, such as Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker of New York University's AI Now Institute have conceptualized "algorithmic impact assessments" to help government agencies or companies to evaluate the accuracy, potential community harms or benefits, and risk of bias or discrimination before deploying automated tools.[90] Bills like the Algorithmic Accountability Act, which Rep. Yvette Clarke (D-N.Y.) and Sen. Ron Wyden (D-Ore.) reintroduced in February 2022, would also require companies that deploy AI for critical decisions to document the representativeness of their input datasets, sources of data collection, any alternatives or considerations to the input data, and overall methodology.[91] In any framework to evaluate the use of facial recognition or other surveillance tools, impact assessments will be critical to help users and developers audit algorithms for accuracy and racial equity both in development and in the context of application. More importantly, the private sector cannot be the sole arbiter of truth when it comes to the performance of these systems; law enforcement must evaluate products and services to anticipate potential privacy risks and actively examine the inclusivity of datasets and potential risks of replicating patterns of marginalization.

From this review, it is clear that facial recognition and surveillance technologies have shifted the balance of power toward law enforcement agencies. That is why privacy protections are more important than ever for all Americans—and they are especially so for the communities of color that may suffer the greatest consequences from their absence.

The authors would like to thank Samantha Lai for editing assistance, Emily Skahill for research support, and Cameron Kerry and Darrell West for feedback and comments. The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars. Amazon, Apple, Facebook, Google, IBM, and Microsoft provide general, unrestricted support to the Institution. The findings, interpretations, and conclusions in this report are not influenced by any donation. Brookings recognizes that the value it provides is in its absolute commitment to quality, independence, and impact. Activities supported by its donors reflect this commitment.

FOOTNOTES

1. **1**"Federal Bureau of Investigation (FBI)," Stanford University, The Martin Luther King, Jr. Research and Education Institute, accessed February 24, 2022, https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi; Alvaro M. Bedoya, "What the FBI's Surveillance of Martin Luther King Tells Us About the Modern Spy Era," Slate Magazine, January 18, 2016,https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html; Virgie Hoban, "'Discredit, Disrupt, and Destroy': FBI Records Acquired by the Library Reveal Violent Surveillance of Black Leaders, Civil Rights Organizations," University of California, Berkeley Library News, accessed February 24, 2022,https://news.lib.berkeley.edu/fbi; Sam Briger, "Documentary Exposes How The FBI Tried To Destroy MLK With Wiretaps, Blackmail," NPR, January 18, 2021,https://www.npr.org/2021/01/18/956741992/documentary-exposes-how-the-fbi-tried-to-destroy-mlk-with-wiretaps-blackmail. (Back to top)
2. **2**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/. (Back to top)
3. **3**Kevin Rector and Alison Knezevich, "Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates," The Baltimore Sun, October 18, 2016,https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html; Shira Ovide, "A Case for Banning Facial Recognition," The New

York Times, June 9, 2020,https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html.
(Back to top)

4. **4**Zolan Kanno-Youngs, "U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance," The New York Times, June 19, 2020,https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html.
(Back to top)
5. **5**"Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," U.S. Department of Justice, July 31, 2020,https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related; Ryan Lucas, "The Justice Department is ending its controversial China Initiative," NPR, February 23, 2022,https://www.npr.org/2022/02/23/1082593735/justice-department-china-initiative.
(Back to top)
6. **6**Michael German and Alex Liang, "Why Ending the Justice Department's 'China Initiative' Is Vital to U.S. Security," Just Security, January 3, 2022,https://www.justsecurity.org/79698/why-ending-the-justice-departments-china-initiative-is-vital-to-u-s-security/; Matt Apuzzo, "U.S. Drops Charges That Professor Shared Technology With China," The New York Times, September 11, 2015, https://www.nytimes.com/2015/09/12/us/politics/us-drops-charges-that-professor-shared-technology-with-china.html; Don Lee, "Why Trump's Anti-Spy 'China Initiative' Is Unraveling," Los Angeles Times, September 16, 2021, https://www.latimes.com/politics/story/2021-09-16/why-trump-china-initiative-unraveling; Emma Coffey, "University Offers to Reinstate Professor Acquitted of Espionage Charges," University of Texas, The Daily Beacon, October 29, 2021,https://www.utdailybeacon.com/campus_news/academics/university-offers-to-reinstate-professor-acquitted-of-espionage-charges/article_f6d0aabe-38ee-11ec-9c23-57a37bddf43c.html; Nicole Perlroth, "Accused of Spying for China, Until She Wasn't," The New York Times, May 9, 2015, https://www.nytimes.com/2015/05/10/business/accused-of-spying-for-china-until-she-wasnt.html.
(Back to top)
7. **7**Nina Wallace, "Of Spies and G-Men: How the U.S. Government Turned Japanese Americans into Enemies of the State," Densho: Japanese American Incarceration and Japanese Internment, September 29, 2017, https://densho.org/catalyst/of-spies-and-gmen/; Pedro A. Loureiro, "Japanese Espionage and American Countermeasures in Pre—Pearl Harbor California," The Journal of American-East Asian Relations 3, no. 3 (1994): 197–210, https://www.jstor.org/stable/23612532; "Statement - The Japanese American Citizens League," American Civil Liberties Union, accessed February 24, 2022, https://www.aclu.org/other/statement-japanese-american-citizens-league; Lori Aratani, "Secret Use of Census Info Helped Send Japanese Americans to Internment Camps in WWII," The Washington Post, April 3, 2018, https://www.washingtonpost.com/news/retropolis/wp/2018/04/03/secret-use-of-census-info-helped-send-japanese-americans-to-internment-camps-in-wwii/.
(Back to top)
8. **8**Alvaro M. Bedoya, "What the FBI's Surveillance of Martin Luther King Tells Us About the Modern Spy Era," Slate Magazine, January 18, 2016, https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-

luther-king-says-about-modern-spying.html; Adam Goldman and Matt Apuzzo, "NYPD Muslim Spying Led to No Leads, Terror Cases," The Associated Press, August 21, 2012, https://www.ap.org/ap-in-the-news/2012/nypd-muslim-spying-led-to-no-leads-terror-cases; Adam Goldman and Matt Apuzzo, "With Cameras, Informants, NYPD Eyed Mosques," The Associated Press, February 23, 2012, https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques.
(Back to top)

9. **9**"U.S. Muslims Concerned About Their Place in Society, but Continue to Believe in the American Dream," Pew Research Center, Religion & Public Life Project, July 26, 2017,https://www.pewforum.org/2017/07/26/findings-from-pew-research-centers-2017-survey-of-us-muslims/.
(Back to top)
10. **10**Tatiana Walk-Morris, "What to Do If You Face Anti-Muslim Discrimination at Airport Security," Vice, September 10, 2021, https://www.vice.com/en/article/epnwjz/what-to-do-if-you-face-anti-muslim-discrimination-islamophobia-at-airport-security.
(Back to top)
11. **11**Adam Goldman and Matt Apuzzo, "NYPD Muslim Spying Led to No Leads, Terror Cases," The Associated Press, August 21, 2012, https://www.ap.org/ap-in-the-news/2012/nypd-muslim-spying-led-to-no-leads-terror-cases; Mike Ahlers and Jeanne Meserve, "Muslim-American Group Criticizes TSA Plan as Profiling," CNN, January 4, 2010, http://www.cnn.com/2010/CRIME/01/04/tsa.measures.muslims/index.html.
(Back to top)
12. **12**John Davis, "Walls Work," U.S. Customs and Border Protection, accessed February 24, 2022, https://www.cbp.gov/frontline/border-security; McKenzie Funk, "How ICE Picks Its Targets in the Surveillance Age," The New York Times, October 2, 2019, https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html; Emma Li, "Mass and Intrusive Surveillance of Immigrants Is an Unacceptable Alternative to Detention," Center for Democracy and Technology (blog), August 5, 2021, https://cdt.org/insights/mass-and-intrusive-surveillance-of-immigrants-is-an-unacceptable-alternative-to-detention/.
(Back to top)
13. **13**Brad Heath, "U.S. Secretly Tracked Billions of Calls for Decades," USA TODAY, April 7, 2015, https://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/; Alvaro M. Bedoya, "What the FBI's Surveillance of Martin Luther King Tells Us About the Modern Spy Era," Slate Magazine, January 18, 2016, https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html.
(Back to top)
14. **14**Andrew Guthrie Ferguson, "Facial Recognition and the Fourth Amendment," Minnesota Law Review 3204 (2021), https://scholarship.law.umn.edu/mlr/3204.
(Back to top)
15. **15**Katelyn Ringrose, "Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns," Virginia Law Review Online 105 (2019): 57, https://www.virginialawreview.org/articles/law-enforcements-pairing-facial-recognition-technology-body-worn-cameras-escalates/.
(Back to top)
16. **16**"Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees," U.S. Government Accountability Office, July 13, 2021, https://www.gao.gov/products/gao-21-105309; Clare Garvie,

Alvaro Bedoya, and Jonathan Frankle, “The Perpetual Line-Up: Unregulated Police Face Recognition in America,” Georgetown Law, Center on Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/.
(Back to top)

17. **17**Kashmir Hill, “The Secretive Company That Might End Privacy as We Know It,” The New York Times, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
(Back to top)
18. **18**Eli Watkins, “Watchdog Says FBI Has Access to More than 641 Million ‘Face Photos’,” CNN, June 4, 2019, https://www.cnn.com/2019/06/04/politics/gao-fbi-face-photos/index.html; Will Knight, “Clearview AI Has New Tools to Identify You in Photos,” Wired, October 4, 2021, https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/.
(Back to top)
19. **19**Max Rivlin-Nadler, “How ICE Uses Social Media to Surveil and Arrest Immigrants,” The Intercept, December 22, 2019, https://theintercept.com/2019/12/22/ice-social-media-surveillance/.
(Back to top)
20. **20**Conor Friedersdorf, “An Unprecedented Threat to Privacy,” The Atlantic, January 27, 2016, https://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/.
(Back to top)
21. **21**"Facial Recognition Technology: Current and Planned Uses by Federal Agencies,” U.S. Government Accountability Office, August 24, 2021, https://www.gao.gov/products/gao-21-526; “Vigilant FaceSearch – Facial Recognition System,” Motorola Solutions, accessed February 24, 2022, https://www.motorolasolutions.com/en_us/products/command-center-software/analysis-and-investigation/vigilant-facesearch-facial-recognition-system.html.
(Back to top)
22. **22**Joseph Cox, “Tech Firm Offers Cops Facial Recognition to ID Homeless People,” Vice, February 8, 2022, https://www.vice.com/en/article/wxdp7x/tech-firm-facial-recognition-homeless-people-odin.
(Back to top)
23. **23**Jeffrey Dastin, “Amazon Extends Moratorium on Police Use of Facial Recognition Software,” Reuters, May 18, 2021,https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/.
(Back to top)
24. **24**Sara Morrison, “Here’s How Police Can Get Your Data — Even If You Aren’t Suspected of a Crime,” Vox, July 31, 2021, https://www.vox.com/recode/22565926/police-law-enforcement-data-warrant.
(Back to top)
25. **25**Matt O’Brien and Michael Liedtke, “How Big Tech Created a Data ‘treasure Trove’ for Police,” AP News, June 22, 2021, https://apnews.com/article/how-big-tech-created-data-treasure-trove-for-police-e8a664c7814cc6dd560ba0e0c435bf90.
(Back to top)
26. **26**Sara Morrison, “A Surprising Number of Government Agencies Buy Cellphone Location Data. Lawmakers Want to Know Why,” Vox, December 2,

2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel; Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," Vice, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.
(Back to top)

27. **27**Jon Keegan and Alfred Ng, "There's a Multibillion-Dollar Market for Your Phone's Location Data," The Markup, September 30, 2021, https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data; Byron Tau and Michelle Hackman, "Federal Agencies Use Cellphone Location Data for Immigrant Enforcement," The Wall Street Journal, February 7, 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.
(Back to top)
28. **28**Max Rivlin-Nadler, "How ICE uses social media to surveil and arrest immigrants," The Intercept, December 22, 2019, https://theintercept.com/2019/12/22/ice-social-media-surveillance/; "Social media surveillance by Homeland Security Investigations: A threat to immigrant communities and free expression," Brennan Center for Justice, November 15, 2019, https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-homeland-security-investigations-threat.
(Back to top)
29. **29**Max Rivlin-Nadler, "How ICE Uses Social Media to Surveil and Arrest Immigrants," The Intercept, December 22, 2019, https://theintercept.com/2019/12/22/ice-social-media-surveillance/; Mary Pat Dwyer and José Guillermo Gutiérrez, "Documents Reveal LAPD Collected Millions of Tweets from Users Nationwide," Brennan Center for Justice, December 15, 2021, https://www.brennancenter.org/our-work/analysis-opinion/documents-reveal-lapd-collected-millions-tweets-users-nationwide.
(Back to top)
30. **30**Matthew Guariglia, "How Are Police Using Drones?" Electronic Frontier Foundation, January 6, 2022, https://www.eff.org/deeplinks/2022/01/how-are-police-using-drones.
(Back to top)
31. **31**Faine Greenwood, "The Chula Vista, California, Police Department's One-of-a-Kind Drone Program," Slate Magazine, May 17, 2021, https://slate.com/technology/2021/05/chula-vista-police-drone-program.html.
(Back to top)/li>
32. **32**Dawn Kawamoto, "Cops Wearing Cameras: What Happens When Privacy and Accountability Collide?" GovTech, accessed February 24, 2022, https://www.govtech.com/biz/Cops-Wearing-Cameras-What-Happens-When-Privacy-and-Accountability-Collide.html; Bryce C. Newell, "Body Cameras Help Monitor Police but Can Invade People's Privacy," The Conversation, May 25, 2021, http://theconversation.com/body-cameras-help-monitor-police-but-can-invade-peoples-privacy-160846; Jennifer Lee, "Will Body Cameras Help End Police Violence?" ACLU of Washington, June 7, 2021, https://www.aclu-wa.org/story/%C2%A0will-body-cameras-help-end-police-violence%C2%A0; German Lopez, "The Failure of Policy Body Cameras," Vox, July 21, 2017, https://www.vox.com/policy-and-politics/2017/7/21/15983842/police-body-cameras-failures.
(Back to top)

33. **33**Rani Molla, "The Rise of Fear-Based Social Media like Nextdoor, Citizen, and Now Amazon's Neighbors," Vox, May 7, 2019, https://www.vox.com/recode/2019/5/7/18528014/fear-social-media-nextdoor-citizen-amazon-ring-neighbors; Jessi Hempel, "For Nextdoor, Eliminating Racism Is No Quick Fix," Wired, February 16, 2017, https://www.wired.com/2017/02/for-nextdoor-eliminating-racism-is-no-quick-fix/.
(Back to top)
34. **34**Rani Molla, "Amazon Ring Sales Nearly Tripled in December despite Hacks," Vox, January 21, 2020, https://www.vox.com/recode/2020/1/21/21070402/amazon-ring-sales-jumpshot-data; Thorin Klosowski, "Facial Recognition Is Everywhere. Here's What We Can Do About It," The New York Times Wirecutter (blog), July 15, 2020, https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.
(Back to top)
35. **35**Lauren Bridges, "Amazon's Ring Is the Largest Civilian Surveillance Network the US Has Ever Seen," The Guardian, May 18, 2021, http://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us; Rani Molla, "How Amazon's Ring Is Creating a Surveillance Network with Video Doorbells," Vox, September 5, 2019, https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell-hacks.
(Back to top)
36. **36**Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," The New York Times, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.
(Back to top)
37. **37**Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Conference on fairness, accountability and transparency: PMLR, 2018, https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
(Back to top)
38. **38**"NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," U.S. National Institute of Standards and Technology, December 19, 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; Natasha Singer and Cade Metz, "Many Facial-Recognition Systems Are Biased, Says U.S. Study," The New York Times, December 19, 2019, https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html; Drew Harwell, "Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use," The Washington Post, December 19, 2019, https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.
(Back to top)
39. **39**"Amazon Rekognition Improves Accuracy of Real-Time Face Recognition and Verification," Amazon Web Services, April 2, 2018, https://aws.amazon.com/about-aws/whats-new/2018/04/amazon-rekognition-improves-accuracy-of-real-time-face-recognition-and-verification/; Brad Smith, "Facial Recognition: It's Time for Action,"

Microsoft On the Issues, December 6, 2018, https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/.
(Back to top)
40. **40**Jon Porter, "Federal Study of Top Facial Recognition Algorithms Finds 'Empirical Evidence' of Bias," The Verge, December 20, 2019, https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon.
(Back to top)
41. **41**Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," The New York Times, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
(Back to top)
42. **42**Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology," Electronic Frontier Foundation, February 12, 2018, https://www.eff.org/wp/law-enforcement-use-face-recognition.
(Back to top)
43. **43**"Criminal Justice Fact Sheet," NAACP, May 24, 2021, https://naacp.org/resources/criminal-justice-fact-sheet.
(Back to top)
44. **44**Laura Moy, "A Taxonomy of Police Technology's Racial Inequity Problems," U. Ill. L. Rev. 139 (2021), http://dx.doi.org/10.2139/ssrn.3340898.
(Back to top)
45. **45**Motion for a European Parliament resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016(INI), European Parliament (adopted 2021), https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html?.
(Back to top)
46. **46**The AI Act, COM/2021/206, European Commission (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.
(Back to top)
47. **47**Anita L. Allen, "Dismantling the 'Black Opticon': Privacy, Race, Equity, and Online Data-Protection Reform," The Yale Law Journal 131, November 16, 2021, https://www.yalelawjournal.org/forum/dismantling-the-black-opticon.
(Back to top)
48. **48**Samuel D. Warren and Louis D. Brandeis, "Right to privacy," Harv. L. Rev. 4 (1890): 193, https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.
(Back to top)
49. **49**Nicandro Iannacci, "Recalling the Supreme Court's Historic Statement on Contraception and Privacy," National Constitution Center, June 7, 2019, https://constitutioncenter.org/blog/contraception-marriage-and-the-right-to-privacy.
(Back to top)
50. **50**Elizabeth Goitein, "The government can't seize your digital data. Except by buying it," The Washington Post, April 26, 2021, https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/.
(Back to top)
51. **51**Caitlin Chin, "Highlights: Setting Guidelines for Facial Recognition and Law Enforcement," The Brookings Institution (blog), December 9,

2019, https://www.brookings.edu/blog/techtank/2019/12/09/highlights-setting-guidelines-for-facial-recognition-and-law-enforcement/.
(Back to top)
52. **52***Riley v. California,* 573 U.S. 373 (2014). https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.
(Back to top)
53. **53***Carpenter v. United States,* 585 U.S. __ (2018). https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.
(Back to top)
54. **54***Florida v. Riley,* 488 U.S. 445 (1989). https://supreme.justia.com/cases/federal/us/488/445/.
(Back to top)
55. **55**Rebecca Darin Goldberg, "You Can See My Face, Why Can't I? Facial Recognition and Brady," Columbia Human Rights Law Review, April 12, 2021, http://hrlr.law.columbia.edu/hrlr-online/you-can-see-my-face-why-cant-i-facial-recognition-and-brady/.
(Back to top)
56. **56***Willie Allen Lynch v. State of Florida* (2018). https://cases.justia.com/florida/first-district-court-of-appeal/2018-16-3290.pdf?ts=1545938765; Aaron Mak, "Facing Facts," Slate, January 25, 2019, https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html.
(Back to top)
57. **57***Long Lake Township v. Todd Maxon and Heather Maxon* (2021). https://www.courts.michigan.gov/siteassets/case-documents/uploads/OPINIONS/FINAL/COA/20210318_C349230_47_349230.OPN.PDF; Matthew Feeney, "Does the 4th Amendment Prohibit Warrantless Drone Surveillance?" Cato Institute, March 24, 2021, https://www.cato.org/blog/does-4th-amendment-prohibit-warrantless-drone-surveillance.
(Back to top)
58. **58**"Electronic Communications Privacy Act (ECPA)," Electronic Privacy Information Center, accessed February 24, 2022, https://epic.org/ecpa/.
(Back to top)
59. **59**Elizabeth Goitein, "How the CIA Is Acting Outside the Law to Spy on Americans," Brennan Center for Justice, February 15, 2022, https://www.brennancenter.org/our-work/analysis-opinion/how-cia-acting-outside-law-spy-americans; "'Incidental,' Not Accidental, Collection," Electronic Frontier Foundation, October 2, 2017, https://www.eff.org/pages/Incidental-collection.
(Back to top)
60. **60**"States Push Back Against Use of Facial Recognition by Police," US News, May 5, 2021, https://www.usnews.com/news/politics/articles/2021-05-05/states-push-back-against-use-of-facial-recognition-by-police; "General FR / Surveillance Regulation," NYU School of Law, Policing Project, accessed September 24, 2022, https://www.policingproject.org/general-regulations.
(Back to top)
61. **61**"Maine Enacts Strongest Statewide Facial Recognition Regulations in the Country," American Civil Liberties Union, June 30, 2021, https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country.
(Back to top)
62. **62**Kim Lyons, "Minneapolis Prohibits Use of Facial Recognition Software by Its Police Department," The Verge, February 13,

2021, https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy.
(Back to top)

63. **63**Cameron F. Kerry, "Why Protecting Privacy Is a Losing Game Today—and How to Change the Game," The Brookings Institution (blog), July 12, 2018, https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.
(Back to top)
64. **64**"Sears Settles FTC Charges Regarding Tracking Software," Federal Trade Commission, June 4, 2009, https://www.ftc.gov/news-events/press-releases/2009/06/sears-settles-ftc-charges-regarding-tracking-software; "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises," Federal Trade Commission, November 29, 2011, https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep; "FTC Approves Final Order Settling Charges Against Snapchat," Federal Trade Commission, December 31, 2014, https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat; "Retail Tracking Firm Settles FTC Charges It Misled Consumers About Opt Out Choices," Federal Trade Commission, April 23, 2015, https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers.
(Back to top)
65. **65**Cameron F. Kerry and Caitlin Chin, "Hitting Refresh on Privacy Policies: Recommendations for Notice and Transparency," The Brookings Institution (blog), January 6, 2020, https://www.brookings.edu/blog/techtank/2020/01/06/hitting-refresh-on-privacy-policies-recommendations-for-notice-and-transparency/; "Federal Trade Commission 2020 Privacy and Data Security Update," Federal Trade Commission, 2020, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.
(Back to top)
66. **66**Christopher Ward and Kelsey C. Boehm, "Developments in Biometric Information Privacy Laws," Foley & Lardner LLP (blog), June 17, 2021, https://www.foley.com/en/insights/publications/2021/06/developments-biometric-information-privacy-laws.
(Back to top)
67. **67**Julie Brill, "Microsoft Will Honor California's New Privacy Rights throughout the United States," Microsoft On the Issues (blog), November 11, 2019, https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/.
(Back to top)
68. **68**"Privacy & Requests," Clearview AI, accessed February 24, 2022, https://www.clearview.ai/privacy-and-requests.
(Back to top)
69. **69**"Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses, U.S. Government Accountability Office, July 13, 2020, https://www.gao.gov/products/gao-20-522.
(Back to top)
70. **70**Eric Lander and Alondra Nelson, "ICYMI: WIRED (Opinion): Americans Need a Bill of Rights for an AI-Powered World," The White House Office of Science and Technology (blog), October 22, 2021, https://www.whitehouse.gov/ostp/news-

updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/.
(Back to top)
71. **71**"Executive Order On Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," The White House, January 20, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/.
(Back to top)
72. **72**"IRS announces transition away from use of third-party verification involving facial recognition," Internal Revenue Service, February 7, 2022, https://www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition; Alan Rappeport, "I.R.S. Will Allow Taxpayers to Forgo Facial Recognition Amid Blowback," The New York Times, February 21, 2022, https://www.nytimes.com/2022/02/21/us/politics/irs-facial-recognition.html; Rachel Metz, "IRS Halts Plans to Require Facial Recognition For Logging In To User Accounts," CNN Business, February 7, 2022,https://www.cnn.com/2022/02/07/tech/irs-facial-recognition-idme/index.html.
(Back to top)
73. **73**George Floyd Justice in Policing Act of 2021, H.R. 1280, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/1280/text.
(Back to top)
74. **74**Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/senate-bill/2052/text.
(Back to top)
75. **75**Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/2878/text.
(Back to top)
76. **76**Fourth Amendment Is Not For Sale Act, S. 1265, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/senate-bill/1265/text.
(Back to top)
77. **77**Sara Morrison, "Here's How Police Can Get Your Data — Even If You Aren't Suspected of a Crime," Vox, July 31, 2021, https://www.vox.com/recode/22565926/police-law-enforcement-data-warrant.
(Back to top)
78. **78**Daniel E. Bromberg and Étienne Charbonneau, "Americans Want Police to Release Body-Cam Footage. But There's a Bigger Worry," The Washington Post, May 5, 2021, https://www.washingtonpost.com/politics/2021/05/05/americans-want-police-release-bodycam-footage-theres-bigger-worry/.
(Back to top)
79. **79**"State and Local Government," The White House, accessed February 24, 2022, https://www.whitehouse.gov/about-the-white-house/our-government/state-local-government/; Alexis Karteron, "Congress Can't Do Much about Fixing Local Police – but It Can Tie Strings to Federal Grants," The Conversation, June 1, 2021, http://theconversation.com/congress-cant-do-much-about-fixing-local-police-but-it-can-tie-strings-to-federal-grants-159881.
(Back to top)

80. **80**Caitlin Chin, "Highlights: Setting Guidelines for Facial Recognition and Law Enforcement," The Brookings Institution (blog), December 9, 2019, https://www.brookings.edu/blog/techtank/2019/12/09/highlights-setting-guidelines-for-facial-recognition-and-law-enforcement/.
(Back to top)
81. **81**Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Line-Up: Unregulated Police Face Recognition in America," Georgetown Law, Center on Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/appendix/model-police-use-policy.
(Back to top)
82. **82**Ibid. (Back to top)
83. **83**Rashawn Ray, "Policy Steps for Racially-Equitable Policing," Testimony before the Virginia Advisory Committee to the U.S. Commission on Civil Rights, July 16, 2021, https://www.brookings.edu/testimonies/policy-steps-for-racially-equitable-policing/.
(Back to top)
84. **84**Laura Moy, "A Taxonomy of Police Technology's Racial Inequity Problems," U. Ill. L. Rev. 139 (2021), http://dx.doi.org/10.2139/ssrn.3340898.
(Back to top)
85. **85**"Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance," 131 Harv. L. Rev. 1715, 1722 (2018), https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.
(Back to top)
86. **86**Angel Diaz, "Law Enforcement Access to Smart Devices," Brennan Center for Justice, December 21, 2020, https://www.brennancenter.org/our-work/research-reports/law-enforcement-access-smart-devices.
(Back to top)
87. **87**Cameron F. Kerry, John B. Morris, Jr., Caitlin Chin, and Nicol Turner Lee, "Bridging the gaps: A path forward to federal privacy legislation," The Brookings Institution, June 3, 2020, https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/.
(Back to top)
88. **88**Cathy Cosgrove and Sarah Rippy, "Comparison of Comprehensive Data Privacy Laws in Virginia, California and Colorado," International Association of Privacy Professionals, July 2021, https://iapp.org/media/pdf/resource_center/comparison_chart_comprehensive_data_privacy_laws_virginia_california_colorado.pdf; General Data Protection Regulation (2016) https://gdpr-info.eu/; Consumer Online Privacy Rights Act, S. 3195, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/senate-bill/3195; SAFE DATA Act, S. 2499, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/senate-bill/2499.
(Back to top)
89. **89**"Brown Releases New Proposal That Would Protect Consumers' Privacy from Bad Actors," Sherrod Brown, U.S. Senator for Ohio, June 18, 2020, https://www.brown.senate.gov/newsroom/press/release/brown-proposal-protect-consumers-privacy; SAFE DATA Act, S. 2499, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/senate-bill/2499.
(Back to top)

90. **90**Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker, "Algorithmic impact assessments: A practical framework for public agency accountability," AI Now Institute, 2018, https://ainowinstitute.org/aiareport2018.pdf.
(Back to top)
91. **91**"Wyden, Booker and Clarke Introduce Algorithmic Accountability Act of 2022 To Require New Transparency And Accountability For Automated Decision Systems," Ron Wyden, U.S. Senator for Oregon, February 3, 2022, https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-algorithmic-accountability-act-of-2022-to-require-new-transparency-and-accountability-for-automated-decision-systems.
(Back to top)