Saint Louis University Law Journal

Volume 65
Number 4 *Tradeoffs: Technology, Privacy, and the Law (Summer 2021)*

Article 8

2021

Warrants Needed for Biometric Analysis

Ted Claypoole
ted.claypoole@wbd-us.com

WARRANTS NEEDED FOR BIOMETRIC ANALYSIS

TED CLAYPOOLE*

ABSTRACT

This article argues that U.S. courts and legislatures should limit law enforcement application of biometric identification technologies within Constitutional bounds. Specifically, warrant requirements should be enforced for police to use facial recognition artificial intelligence and software. Such warrant requirement is practical for law enforcement and is already within the bounds of current Fourth Amendment cases.

* Partner at Womble Bond Dickinson (US) LLP.

Surveillance creep has engulfed our world. Over the past thirty years the tools for intruding on personal privacy and learning about the thoughts and actions of individual humans have exploded in variety and number.[1] Those tools expand each year and become easier to use and more available to everyone.[2]

Some of this growth stems from the technology we accept into our lives. In 2021, nearly all of us carry or wear tracking devices that can pinpoint our location on the globe.[3] We bring cameras and microphones into our homes and then connect them to the wider world via the internet. The internet itself, through social media, digital shopping, electronic news programs, and self-publishing, carves windows into our feelings, priorities, and preferences that simply did not exist prior to 1990.[4]

Part of the growth in surveillance arises because technology used by companies and law enforcement has improved in a spectacular fashion. Many police departments now use Stingray devices that mimic cell towers to capture the content of phone calls.[5] Others operate self-controlled drones as first responders.[6] Networks of cameras on houses, banks, intersections, and street corners are available for law enforcement to peruse at will. Our vehicles and personal devices will show police where we are, both now and when a crime was committed.[7] Artificial intelligence has advanced to a point where computers can assist in matching license plates, fingerprints, or other identifying information captured.[8]

1. Chris Stobing, *A Brief History of Government Surveillance and Spying and How it Invades Your Privacy*, COMPARITECH, https://www.comparitech.com/vpn/a-brief-history-of-government-surveillance-spying/ [https://perma.cc/YL7V-D6PS] (last updated Jan. 4, 2021).

2. Carly Minsky, '*Surveillance Creep' as Cameras Spread on Campus*, FINANCIAL TIMES (Mar. 10, 2020), https://www.ft.com/content/dd732ab4-3e0a-11ea-b84f-a62c46f39bc2 [https://perma.cc/6ULQ-TCGB].

3. 96% of Americans own mobile phones and 81% own smart phones. *Mobile Fact Sheet*, PEW RES. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/#:~:text=mobile%20revolution%20below.,Mobile%20phone%20ownership%20over%20time,smartphone%20ownership%20conducted%20in%202011 [https://perma.cc/K7TZ-WUZW].

4. Alexandra Rengel, *Privacy-Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights*, 8 INTERCULTURAL HUM. RTS. L. REV. 177, 178–79 (2013).

5. Gregory Maleska, *Stinging the Stingray: The Need for Strong State-Level Anti-Surveillance Legislation*, 52 VAL. U. L. REV. 629, 634 (2017).

6. Cade Metz, *Police Drones are Starting to Think for Themselves*, N.Y. TIMES (Dec. 5, 2020), https://www.nytimes.com/2020/12/05/technology/police-drones.html?action=click&module=Top%20Stories&pgtype=Homepage [https://perma.cc/ZV5Z-842M].

7. Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies in Policing*, 92 N.Y.U. L. REV. ONLINE 19, 22–23 (2017).

8. Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J. L. TECH. & POL'Y 281, 285 (2011).

These trends have arisen in a time where politicians and the general public are particularly wary of placing limits on policing.[9] Since the attacks on the World Trade Center in 2001, Americans have been reluctant to place limits on policing. But that dynamic has changed recently as the Black Lives Matter movement brought law enforcement overreach into the national conversation.[10] However, states still seem wary of blocking police departments from gathering every possible tool available for catching criminals and pursuing potential terror suspects.[11] This has led to a militarization of U.S. police forces[12] and a nearly unchecked ability for law enforcement to adopt powerful new surveillance technologies without preliminary public policy discussion of advisability or even constitutionality.[13] The intrusiveness of these technologies should lead to legislative analysis of whether their application on the citizenry violates Fourth Amendment protections against unlawful search and seizure.

Discussions of what constitutes appropriate search and seizure of electronic information have begun in federal courts,[14] and very recently appeared as a direct ballot initiative in Michigan,[15] but have not broadly spread to state legislatures. Where states and cities have addressed the issue, they have tended to overreact by banning police use of facial recognition technology entirely. For example, several cities have proscribed the use of facial recognition artificial intelligence ("AI") by law enforcement, properly recognizing the constitutional harm threatened in the government application of machine learning software to identify every face in a peaceful political protest.[16] But this extreme restriction

9. *See, e.g.*, Victoria Bekiempis & Adam Gabbatt, *US Cities and States Take Moderate Steps to Reform Police Departments*, THE GUARDIAN (June 9, 2020), https://www.theguardian.com/us-news/2020/jun/09/new-york-police-budget-cut [https://perma.cc/Z942-8322].

10. Kara Dansky, *Local Democratic Oversight of Police Militarization*, 10 HARV. L. & POL'Y REV. 59, 62 (2016).

11. *Id.*

12. *Id.* at 59 ("Furthermore, the American Civil Liberties Union (ACLU) conducted a study in 2014 and found that not only have the police become excessively militarized, but also that police militarization has occurred with little to no public oversight.").

13. Ashley M. Eick, *Forging Ahead from Ferguson: Re-Evaluating the Right to Assemble in the Face of Police Militarization*, 24 WM. & MARY BILL OF RTS. J. 1235 (2016).

14. Joh, *supra* note 7, at 26.

15. MICH. CONST. art. I, § 11 (1963) (as amended by Proposal 2, passed November 3, 2020, requiring a search warrant to access electronic data or electronic communications, and securing electronic data and electronic communications from unreasonable searches and seizures).

16. Danny McDonald, *Boston City Council Unanimously Votes to Ban Use of Face Surveillance Technology by City Government*, BOSTON GLOBE (June 24, 2020, 1:33 PM), https://www.bostonglobe.com/2020/06/24/metro/boston-city-council-unanimously-votes-ban-use-face-surveillance-technology-by-city-government/ [https://perma.cc/93WL-HDE2] (Boston banned facial recognition AI); Rachel Metz, *Portland Passes Broadest Facial Recognition Ban in the U.S.*, CNN (Sept. 9, 2020, 8:06 PM), https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html [https://perma.cc/7XGL-LSDS] (Portland prohibits both public use and private applications in public areas for facial recognition AI); Rachel Metz, *Beyond San Francisco,*

ignores the societal benefit of investigators identifying a person captured on camera throwing a bomb into a building.

This Note proposes that both courts and legislatures should act to limit law enforcement uses of biometric technologies in a manner consistent with the Constitution. Facial recognition software, for example, can be an unconstitutional impingement of search and seizure limitations for people to whom it is applied without suspicion of criminal activity, but the same software can be a constitutionally allowable method of identifying a suspect who was recorded on video committing a crime. Therefore, like all tools, the technology itself is not constitutionally suspect; however, certain applications of the technology may be. The same person can use a hammer to build a home or to murder a neighbor; one application is a benefit and the other a crime. Similarly, unconstitutionally intrusive applications of facial recognition AI software should have legal consequences, not the existence of the tool or the simple fact that law enforcement agencies are using it.

The best way to address this problem is to require police to secure a warrant before applying biometric machine learning software systems to identify people in pictures and videos. This solution is easy to apply in practice and appropriately modernizes the operation of the Fourth Amendment to the United States Constitution to address technologies that could not have been conceived by our founders but affect the rights of citizens every day. Furthermore, a warrant requirement for law enforcement application of this technology falls in line with recent U.S. Supreme Court cases where electronic surveillance has been found unconstitutionally intrusive.[17]

While the Supreme Court seems to be moving in this direction, that path is long and uncertain. It can take years for the appropriate case to wind its way through the U.S. federal appellate system, and a case with an unusual fact pattern can affect the breadth of a decision and the clarity of its application. Often the Supreme Court will wait for a split in federal circuits before it will rule on a matter. Yet facial recognition databases are continuously growing, and the technology is engaged regularly by law enforcement agencies at all levels across

More Cities are Saying No to Facial Recognition, CNN (July 17, 2019, 5:11 PM), https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html [https://perma.cc/QCS7-VKVZ] (Oakland banned any government agency from using facial recognition software); Xiumei Dong, *San Fransico Bans Facial Recognition Technology Surveillance*, Law.com (May 14, 2019, 7:17 PM), https://www.law.com/therecorder/2019/05/14/san-francisco-bans-facial-recognition-technology-surveillance/?slreturn=20210227152702 [https://perma.cc/C2LD-9SY4] (San Francisco passed "Stop Secret Surveillance" ordinance completely banning any city agency's use of facial surveillance).

17. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); Riley v. California, 573 U.S. 373, 403 (2014).

the country.[18] Therefore, legislatures should act now to place practical limits on the application of facial recognition programs by police.

I. OBTAINING A WARRANT IS PRACTICAL FOR LAW ENFORCEMENT

Since the founding of our Republic,[19] police have been required to secure a warrant to search the person, home, and papers of citizens whenever reasonably practicable.[20] The Supreme Court held "this rule rests upon the desirability of having magistrates rather than police officers determine when searches and seizures are permissible and what limitation should be placed upon such activities."[21] This is the streamlined system all of our policing agencies use when they want to go somewhere or do something that might otherwise intrude on the Fourth Amendment right to be secure in our persons, homes, and papers.[22] The

18. *See* CONGRESSIONAL RESEARCH SERVICE, FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY (Oct. 27, 2020), https://fas.org/sgp/crs/misc/R46586.pdf [https://perma.cc/C5LE-YAFX] ("The [FBI] operates two programs that support the use of the technology: (1) the Next Generation Identification–Interstate Photo System (NGI-IPS), largely supporting state and local law enforcement; and (2) the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit, supporting FBI investigations. NGI-IPS contains criminal mugshots, and the system allows authorized law enforcement users (primarily state and local) to search the database for potential investigative leads. The FACE Services Unit supports FBI investigations by searching probe photos of unknown persons against faces in NGI-IPS and other federal and state facial recognition systems authorized for FBI use.").

19. An early statement of freedom from unreasonable searches and seizures appeared in The Rights of the Colonists and a List of Infringements and Violations of Rights, 1772, in the drafting of which Samuel Adams took the lead. B. SCHWARTZ, THE BILL OF RIGHTS: A DOCUMENTARY HISTORY 199, 205–06 (1971). Cornell's annotation of the Fourth Amendment also includes the following discussion of how early Colonial leaders became concerned about overbroad searches and seizures:

> In order to enforce the revenue laws, English authorities made use of writs of assistance, which were general warrants authorizing the bearer to enter any house or other place to search for and seize "prohibited and uncustomed" goods, and commanding all subjects to assist in these endeavors. Once issued, the writs remained in force throughout the lifetime of the sovereign and six months thereafter. When, upon the death of George II in 1760, the authorities were required to obtain the issuance of new writs, opposition was led by James Otis, who attacked such writs on libertarian grounds and who asserted the invalidity of the authorizing statutes because they conflicted with English constitutionalism. Otis lost and the writs were issued and used, but his arguments were much cited in the colonies not only on the immediate subject but also with regard to judicial review.

Legal Information Institute, *History and Scope of the Fourth Amendment*, CORNELL LAW SCHOOL, https://www.law.cornell.edu/constitution-conan/amendment-4/history-and-scope-of-the-amendment#fn7amd4 [https://perma.cc/B4UF-KEVR].

20. Chimel v. California, 395 U.S. 752, 761 (1969) ("The [Fourth] Amendment was in large part a reaction to the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence. In the scheme of the Amendment, therefore, the requirement that 'no Warrants shall issue, but upon probable cause,' plays a crucial part.").

21. *Id.* at 758.

22. U.S. CONST. amend. IV.

officer simply needs to show that she has a reasonable suspicion that a person has committed a crime, and then the officer is issued a warrant that allows intrusion on private spaces and information.[23] The process is simple, and a warrant should be easy to obtain with clear indications that a specific individual may have committed a crime.[24]

In 1967, Justice Harlan observed that, with regard to the government's use of an advanced wiretapping technique, "[a]s elsewhere under the Fourth Amendment, warrants are the general rule, to which the legitimate needs of law enforcement may demand specific exceptions."[25] This keeps our police force from searching everyone and everything hoping to find something to support an arrest. That's why the protection was written into the Constitution by our nation's founders. The warrant requirement is meant to slow the process down so that someone can think about whether the one group in society with a legal monopoly on violence should be crashing through your front door and rifling through your underwear drawer.

Police already have the correct forms to fill. They know how the process works. Judges are addressing these matters all the time. In other words, the only extra time required in obtaining a warrant to apply facial recognition AI to a set of public pictures will be the extra time that police are *supposed* to take when they intrude on a person's privacy. Requiring a warrant in these cases will not change the way law enforcement operates now on actions that intrude on privacy and will not change the manner that police are supposed to be operating.

II. REQUIRING A WARRANT FOR POLICE TO RUN FACIAL RECOGNITION SOFTWARE WOULD PROTECT OUR CONSTITUTIONAL RIGHTS

Facial recognition software can be used for purposes that some people would find violative of Fourth Amendment protections against improper searches. The Supreme Court has held that U.S. citizens have a right to remain anonymous in their political activity,[26] stating "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[27] Indiscriminate or politically targeted applications of facial recognition software searching politically motivated crowds could violate that right. The ability to focus on face after face, revealing name after name, must be

23. Legal Information Institute, *supra* note 19.

24. Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 643 (1989) (Marshall, J., dissenting); Walter v. United States, 447 U.S. 649, 657 (1980).

25. Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).

26. NAACP v. State of Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958) (stating that "compelled disclosure of affiliation with groups engaged in advocacy may constitute" serious restraints on First Amendment rights).

27. *Id.*

examined for constitutionality unless the government's motivation clearly falls within permissible search parameters.

We can start with an example where an American crowd was lawfully demonstrating against the police force itself—this could be because the police are enforcing restrictive gun laws or because of a discriminatory use of force. Every group in the political spectrum could have a reason to protest law enforcement policies or behaviors. For centuries, demonstrators have relied on the anonymity of a crowd to protect them from government retaliation. Technology makes today's world different. Police can scan the crowd using cameras in place for traffic control or business security, cameras worn by uniformed officers or wielded by members of the crowd itself, or even sent over the demonstration on drones.[28] They can save and store the pictures to study at a later date. None of these activities would likely surprise or escape the notice of people marching that day.

But those marchers would likely be surprised that local law enforcement has the ability to apply an AI program driven by an enormous database of photographs tied to the names of pictured people.[29] They would not expect that by simply marching in a political demonstration, police could quickly develop a list of people who supported the day's cause and use that list for any reason without the need to explain this activity to anyone in authority.[30] In this manner, police could develop 'enemy lists' of citizens who protested the activities of law enforcement and settle scores with these people later. In other words, protesting citizens have a reasonable expectation of not being identified and later harassed by police, otherwise the citizens might choose not to participate in the protests and expose themselves to the later reprisals from angry government officials.

As U.S. Supreme Court Justice Sonia Sotomayor, quoting Judge Flaum of the Seventh Circuit, noted:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[31]

28. Aaron Holmes, *How Police are Using Technology Like Drones and Facial Recognition to Monitor Protests and Track People Across the US*, BUS. INSIDER (June 1, 2020), https://www.businessinsider.com/how-police-use-tech-facial-recognition-ai-drones-2019-10#cell-tower-simulators-or-stingrays-5 [https://perma.cc/LSP4-ZQDX].

29. Stobing, *supra* note 1.

30. *See* Holmes, *supra* note 28.

31. Jones v. United States, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas–Perez*,* 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

Judge Flaum wrote in 2011 about tracking a person's body constantly everywhere it goes.[32] He was commenting on new technology enabling law enforcement to gather information all at once in a manner that for the rest of the country's history would have involved extensive police resources.[33] The judge was observing that, where a police agency could now perform a task with a touch of a button that once would have taken dozens of officers and tens of thousands of dollars, that new dynamic should be evaluated as to whether it constituted an unreasonable search.[34] The same logic also applies to technology that allows police to not only see all the people in a given space at any particular time, but to apply names to all the faces that appear there.

Just like around-the-clock tracking technology, facial recognition software applied by the government clearly "alters the relationship" between police and citizens.[35] Changes in technology have been adopted by law enforcement for at least 150 years and have shifted the nature of the relationship between government and citizenry. When photography was introduced, mug shots made identifications much easier. Electric lights facilitated searches. Replacing horses with automobiles not only made long-distance travel easier, but the automobile became a new stage to conduct personal searches. The application of inexpensive listening and recording devices allowed deeper intrusion into the lives of witnesses and suspects.[36] Computers, lapel cameras, drones, stingrays, military hardware, and AI databases containing boundless biometric identification markers for speech, faces, and DNA all change the nature of policing.[37] For a century, U.S. judges have noted how technological changes may affect constitutional rights. In his famous 1928 dissent, Justice Brandeis noted the march of technology and its effect on Fourth Amendment rights, writing:

> Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack to obtain disclosure in court of what is whispered in the closet. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Moreover, "in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be." The progress of science in

32. *See* United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Wood, J., dissenting).

33. *Id.*

34. *Id.*

35. Jay Greene, *Microsoft Won't Sell Police its Facial-recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [https://perma.cc/6C75-FAQJ].

36. *See* Katz v. United States, 389 U.S. 347, 362 (1967).

37. Theodore Claypoole, *A Clear Solution to Police Surveillance Creep: Warrants Needed for Biometric Analysis*, AM. BAR ASS'N (Aug. 3, 2020), https://www.americanbar.org/groups/business_law/publications/blt/2020/08/police-surveillance/ [https://perma.cc/K42F-CZVT].

> furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[38]

In 2001, a unanimous Supreme Court found that the "advance of technology" clearly affects "the degree of privacy secured by citizens under the Fourth Amendment," observing that human flight had made previously private spaces more vulnerable to observation.[39]

More recently, as the pace of technological advancement has increased, the court has addressed its intrusion on constitutional rights more frequently. For example, Justice Scalia wrote, "[a]pplying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice."[40] This is because we must "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[41] If the technology allows law enforcement to intrude deeply into our lives in new ways that would have been unimagined 250 years ago, it must be checked by the Fourth Amendment—requiring police to obtain a warrant before using the intrusive technology.

When we apply this thinking to facial recognition database technology, we can require a warrant be issued to seek the identity of obvious wrongdoers. So, if a person is caught on camera throwing a Molotov cocktail through a plate glass window, the police can clearly and easily use a facial recognition program to find that person and bring them to justice. But if one simply walks in a peaceful political demonstration, the police would not be allowed to run facial recognition software to place them in the crowd at that time. Except for the few cities who have directly proscribed its use, under current U.S. law with no warrant requirement, law enforcement can currently run the biometric identification program without limitations.

III. THE U.S. SUPREME COURT'S RECENT OPINIONS SUPPORT A WARRANT REQUIREMENT FOR POLICE TO APPLY FACIAL RECOGNITION SOFTWARE

The Supreme Court has already begun to move toward this conclusion, insisting on Fourth Amendment protections for transformative technologies, requiring a warrant for law enforcement to place a thirty-day tracking beacon on a personal vehicle[42] and insisting that a warrant is needed to open and review

38. Olmstead v. United States, 277 U.S. 438, 474 (1928).
39. Kyllo v. United States, 533 U.S. 27, 33–34 (2001).
40. City of Ontario v. Quon, 560 U.S. 746, 768 (2010).
41. *Kyllo*, 533 U.S. at 33–34 (2001).
42. Jones v. United States, 565 U.S. 400, 404 (2012).

the contents of a citizen's smartphone.[43] Extending the protection of digital privacy against random searches and seizures, the Court even held that police need a warrant to request from relevant service providers historic cell phone tracking records to pinpoint your location at different times in the past.[44] This latter decision extended an exception to decades of precedent protecting the concept that allowing a third party to create, access or hold private records destroys an individual's Fourth Amendment right to protect those records from government search and seizure.[45]

Seventy years ago the Supreme Court held that keeping one's name from being associated with political causes was a part of the right to free speech and free association.[46] There may be reason to fear the government taking note of such association, which is why the Supreme Court decided that the State of Alabama in the 1950s was not allowed to require the local NAACP chapter to produce a list of all of its members, placing each member at physical risk.[47] Using current technology, the State of Alabama would not need to analyze membership lists, but could capture video of everyone entering meetings and apply facial recognition software to entire group, finding the names it seeks with the push of a button. This AI could also allow government enforcement officers to not only see who is entering gay bars, gun clubs, and political protests, but then to identify each individual. Clearly the technology, if randomly or maliciously applied, could invade or chill people's speech and assembly rights.

In the past decade, the Supreme Court has extended its concern expressed in the NAACP case to protect the privacy of individuals even in public places. In the recent smart phone data accessibility case of *Carpenter v. U.S.*—confirming that protection from unlawful search and seizure extends well beyond the home of a protected party—Chief Justice John Roberts wrote, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."[48] To the contrary, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[49] Roberts then noted how technology has changed the calculation of what should be considered a reasonable expectation of privacy even in the public sphere, writing, "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection . . . [with current technology] police need

43. Riley v. California, 573 U.S. 373, 403 (2014).

44. Carpenter v. United States, 138 S. Ct. 2206, 2220–21 (2018).

45. *Id.* at 2220 (extending exceptions to the third-party doctrine initially raised in United States v. Miller, 425 US 435 (1976)); *Riley*, 573 U.S. at 403.

46. NAACP v. State of Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958).

47. *Id.* at 466.

48. 138 S. Ct. at 2217.

49. *Id.*

not even know in advance whether they want to follow a particular individual, or when."[50]

The court has recognized that anonymously attending sensitive political meetings is an important right covered by the First Amendment, and that limited technological intrusions on privacy is an important value of the Fourth Amendment. Facial recognition software, where used indiscriminately by police, seems to run afoul of both of these constitutional values recognized by the Court. The new technology of machine-learning facial recognition software, like the global positioning system data or cell phone triangulation information pulled from a citizen's smartphone, holds the potential to reveal both private and constitutionally protected aspects of a person's life.

The Court in the *Carpenter* case decided that the always-there mobility plus the deep trove of information carried by the smartphone demanded a different Fourth Amendment analysis than stationary telephones, and that individuals maintain legitimate expectations of privacy in the record of their physical movements as captured through cell phone records, even if those movements were taken through public spaces where anyone could see the individual.[51] So, individuals congregated in a politically active crowd should not lose such protections from intrusive technology simply because the crowd had made its point in the public sphere. Harkening back to one of the first Supreme Court discussions of privacy rights in a Fourth Amendment context, the court wrote:

> As Justice Brandeis explained in his famous dissent, the Court is obligated—as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections. Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, "after consulting the lessons of history," drafted the Fourth Amendment to prevent.[52]

Using precisely the same logic, the powerful new technological tool of artificial intelligence driven facial recognition software can be used to carry out important responsibilities for the government, while some of its abuses are the same type—indiscriminate or punitive searches—that the founders drafted the Fourth Amendment to prevent. As the Court decided in *Carpenter*, the obvious solution to this technologic and constitutional quandary is to require the police to apply for and receive a warrant to use the potentially risky technology.[53]

When will application of the technology rise to a level that a warrant is required? The Court, in the recent *Kyllo* decision, held that "a Fourth

50. *Id.* at 2218.

51. *Id.* at 2217.

52. *Id.* at 2223 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

53. *Carpenter*, 138 S. Ct. at 2223.

Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[54] Just like the concerns of the NAACP who wished to keep their membership rolls from access by the State of Alabama in the 1950s, it seems reasonable that modern peaceful political protesters could subjectively fear being named to police or unsympathetic government officials if they are identified by name during political gatherings. For this reason, unregulated application of facial recognition technology may well violate the Supreme Court's conception of the Fourth Amendment prohibition against unreasonable search.

The Supreme Court recently addressed this precise question. In her concurrence to the long-term surveillance case of *United States v. Jones*, Justice Sotomayor proposed:

> I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of [new technology] through lawful conventional surveillance techniques . . . I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance.[55]

Using new technology to identify anyone and everyone occupying visible spaces is the ultimate example of "permeating police surveillance." Facial recognition software, when combined with the current growing omnipresence of surveillance video in metropolitan areas, enables this exercise of police power more than any tool we have ever known.

The most defensible constitutional choice in this circumstance is for Congress or multiple state legislatures to place limits on policing power by requiring warrants to run biometric identification software. Several Justices seem to agree, as they joined Justice Alito in his concurrence in *Jones*, where he wrote:

> In the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken . . . In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.[56]

54. Kyllo v. United States, 533 U.S. 27, 33 (2001).

55. Jones v. United States, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring).

56. *Id.* at 429 (Alito, J., concurring).

In November of last year, U.S. Senators Coons and Lee introduced bi-partisan legislation requiring federal law enforcement to obtain a court order before using facial recognition technology.[57] This bill provided a logical framework for protecting Americans from a powerful new state-operated technology that has grown unchecked as a tool for intruding on citizens' privacy.

Since that time, the Facial Recognition and Biometric Moratorium Act was introduced into both houses of Congress this summer.[58] The Act calls for a complete prohibition on police use of facial recognition software and similar biometric technology like voice recognition or gait identification systems.[59] However, this act, like some of the city-level bans that have been enacted in the United States, overreacts to the availability of this technology. Biometric identification tools are valid and useful law enforcement implements, so banning them removes an important field of investigation for police. The tool is not the constitutional problem. Indiscriminate police application of the tool is the problem.

But requiring a warrant to use the powerful technologies stops indiscriminate and hostile political applications, while maintaining the software's availability to help catch criminals. Warrant obligations are the right step to protect our privacy and other constitutional rights while applying the technology to important problems. We should not wait for the right case to rise to the Supreme Court before limiting use of this technology. A legislative solution is best and fastest.

57. S. 2878, 116th Congress (2019–2020).

58. *See generally* H.R. Res. 7356, 116th Cong. (2019–2020).

59. *Id.* at § 3(a).