Written Testimony of Professor Andrew Guthrie Ferguson

Before the House of Representatives Committee

on Oversight and Reform

Hearing On:

Facial Recognition Technology: (Part 1)

Its Impact on our Civil Rights and Liberties

May 22, 2019

Chairman Cummings, Ranking Member Jordan, and Members of the Committee, thank you for the opportunity to testify today.

I am a law professor who studies the intersection of big data policing technologies and Fourth Amendment freedoms.[1] For the past decade I have been studying how new surveillance technologies shape constitutional rights and police powers.[2] Based on that expertise, I have a very simple message today:

Congress should act to regulate new facial recognition surveillance technologies, because the case-by-case, slow process of Fourth Amendment litigation is inadequate to address the rapidly changing world of mass surveillance.

I will be making five main points.

First, the Fourth Amendment will not save us from the privacy threat posed by facial recognition technology. The Supreme Court is making solid strides in trying to update Fourth Amendment principles in the face of new technology, but they are chasing an accelerating train and will not catch up. Legislation is needed to respond to the real-time threats of real-time technology.

Second, the Fourth Amendment was never meant to be the sole source of government regulation. Instead, our entire constitutional system is premised upon Congress taking a leading role, guided by—and only in the rare instance overruled by—our founding Constitution. Indeed, one Supreme Court Justice in particular—Justice Samuel Alito—has explicitly welcomed Congressional assistance.[3] In *Riley v. California*, Justice Alito stated, "[I]t would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."[4]

Third, the few steps the Supreme Court has made on the subject of locational tracking technologies offer guidance on how to avoid drafting a law that could get struck down on Fourth Amendment grounds. Most recently, the Court struck down provisions of the Stored Communications Act in *Carpenter v. United States*,[5] involving law enforcement acquisition of third-party cell-site records. Such acquisition, held the Court, typically requires a probable-cause

[1] Professor of Law, University of the District of Columbia, David A. Clarke School of Law, Senior Visiting Fellow, Harvard Law School Criminal Justice Policy Program, Technology Fellow, Policing Project at NYU Law School, https://www.law.udc.edu/page/AFerguson.

[2] *See e.g.*, Andrew Guthrie Ferguson, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017).

[3] *Carpenter v. United States*, 138 S. Ct. 2206, 2261 (2018) (Alito, J. dissenting) ("Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope."); *United States v. Jones*, 565 U.S. 400, 427 (2012) (Alito, J. concurring) ("[C]oncern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions.").

[4] *Riley v. California*, 573 U.S. 373, 408 (2014) (Alito, J. concurring in part).

[5] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

warrant.[6] As Congress debates creating standards to regulate facial recognition surveillance technology, this Fourth Amendment floor is a necessary baseline consideration.

Fourth, as Congress builds a scaffolding off that constitutional floor, we need to think about the technology not just though the lens of today, but with an eye toward the expansion of surveillance technologies that will combine, aggregate, link, and share data in ways that will reshape the existing power dynamics of government and the people. We are not just talking about technological hardware – cameras, computers, tools – but systems of surveillance, in particular, big data policing systems that can process, store, and retrieve information in ways that has never been possible in past eras. Legislation should future-proof privacy protections with an eye toward the growing scope, scale, and sophistication of systems of surveillance.

Finally, these Fourth Amendment questions must be coupled with a focus on First Amendment freedoms, civil rights, and fundamental fairness when it comes to public safety protections. The burden of surveillance technology has never been equally shared across socio-economic or racial groups. Surveillance is both a civil rights issue and a civil liberties issue and Congress needs to regulate with racial justice in mind.

And, while I know we are here to talk about facial recognition surveillance technology, I hope you will see that these same issues arise in a host of big data policing technologies involving algorithms, sensor surveillance, and predictive analytics.

My written testimony proceeds as follows. After a brief overview of the challenges raised by facial recognition technology, I offer an examination of potential "use cases" of "face surveillance" and "face recognition" technologies. Next, I provide the Fourth Amendment background of how courts would analyze the technologies, concluding that application of current Fourth Amendment doctrine provides an unsatisfactory and incomplete answer which necessitates a statutory response. I end with concrete legislative recommendations based on Fourth Amendment principles about how Congress should regulate facial recognition technology. As used here "facial recognition" technology is a broad term covering all types of biometric technologies that identify individuals by digitally measuring and matching their faces. "Face surveillance" is defined as the application of that technology to generalized monitoring without individualized suspicion. "Face recognition" is defined as the application of that technology to investigatory identifications with individualized suspicion.

A. Facial Recognition: The Challenge

Facial recognition is game-changing technology that has the ability to erode associational privacy and undermine personal security.[7]

Law professors like to use hypotheticals, so let me provide two that demonstrate why facial recognition should be addressed now and in a bipartisan manner.

[6] *Id.* at 2221 ("Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records.").

[7] Clare Garvie et al., Geo. L. Ctr. on Privacy & Tech., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 1 (2016).

Hypothetical 1: There exists a longstanding debate about the wisdom of gun owner databases. Many gun-rights advocates fear that such centralized lists of gun owners could chill Second Amendment rights. Local law enforcement and local officials have differing views on the subject. But that debate will become moot in jurisdictions that wish to use face surveillance technology to identify gun owners. Want to know who is buying a gun? Put a real-time face surveillance camera outside a gun show or gun store. Or, have the local police put the face recognition camera outside a gun range and search the stored footage for all identifiable faces. Unregulated face recognition will eviscerate the privacy of gun owners seeking to purchase or lawfully use guns. Their faces will identify them and mark them.

Hypothetical 2: There exists a longstanding debate about legal and illegal immigration. Many advocates wish to keep undocumented individuals and asylum applicants from government surveillance, lest they become chilled from obtaining basic legal, medical, and other services. Yet, face recognition technology will eviscerate any ability to obtain information without being identified. A face recognition camera outside a legal services office will chill access. A face recognition camera outside a hospital emergency room will undermine public health.

Now add a fact. Once police have the facial recognition image – gun owner or immigrant – any camera with the appropriate software can find that person across a city. If our gun owner goes to the local high school or bank, a real-time alert system can identify them. If police wanted to find all the times that that particular gun owner's face showed up in a city's network of stored surveillance cameras over time – police could do it. Locational tracking by facial recognition (both real time and using stored footage) is technically possible and raises hard Fourth Amendment questions.

B. Police Use of Facial Recognition

Facial recognition technology is a powerful tool currently without federal regulation. Any legislative response must take into account the different ways police could use the technology. The summary below simplifies the types of police use into three categories: (1) general face surveillance (without individualized suspicion); (2) investigative face recognition (with individualized suspicion); and (3) non-law enforcement or emergency purposes.

1. Generalized Face Surveillance

Generalized face surveillance involves monitoring public places or third-party image sets using facial surveillance technologies to match faces with a prepopulated list of face images held by the government.[8] Currently, no federal law prohibits this type of generalized surveillance using facial recognition technology.

[8] *See generally*, Sharon Nakar, Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 94 (2017) ("Generally the facial recognition systems are designed today to seek out patterns in captured images that compare favorably to facial model. Systems are typically programmed such that when a pattern is found to resemble a facial model, the software generates the assumption that there is a face presented in the photo.").

As a general matter, three forms of surveillance technologies exist in this category: (a) scanning stored surveillance footage to identify all faces in the data; (b) real-time scanning of video surveillance to identify all faces passing by the cameras; and (c) datamining stored images from third party platforms to identify individuals.

a. Face Surveillance: Scanning Stored Surveillance Footage: One potential form of face surveillance is the ability to search stored footage from networked surveillance cameras.[9] These cameras can be government owned, private, or via mobile devices like police-worn body cameras. As digital storage becomes cheaper and more available and as video analytics technology becomes more sophisticated, the vast hours of daily video footage can be data mined for identifiable faces. Face surveillance matches any face in a government dataset to a matching face captured in surveillance data. To be clear, the search in stored footage is not based on an individualized suspicion or for a particular criminal investigation, but merely for generalized monitoring of people as they come into contact with the cameras. The resulting scans could map the location of individuals at any point they are identified by a camera.

b. Face Surveillance: Real-Time Monitoring: Another potential form of face surveillance technology is real-time public monitoring. The technology already exists (and is being used in other countries like China) to watch the streets and identify people in public spaces using pattern matching technology.[10] Imagine a TV monitor of a city street with every human figure digitally framed by a box around his or her face. As they pass by cameras, their personal information displays because the surveillance system has matched a pre-populated face to their real-time presence. Again, in this type of monitoring there is no individualized suspicion of criminal wrongdoing. Generally, the justification for use would be public safety (or social control), for example, to identify all of the people going to a sporting event, or frequenting an entertainment district, or entering a gun show. Cameras can be fixed, mobile, on drones, or privately owned.

c. Face Surveillance: Datamining Third-Party Stored Images: The same type of generalized face surveillance can be done by scanning private photo datasets or private digital images. Billions of images and videos exist in third party systems like Facebook, Google, Instagram, Twitter, YouTube, and other platforms. Acquiring those images and matching them would allow law enforcement to build dossiers of individuals in a community. Again, this type of face surveillance match is not done for a particularized law enforcement purpose but rather to gather information about individuals in the community. The resulting identifications could involve locational details (both in metadata of the photos and from the context/content of the photos themselves), personal connections, likes, interests, and activities. One of the realities of digital photographs is that by design they encode information about location, time, date, camera type, and thus details about where, when, and how the photo was taken.[11]

---

[9] Clare Garvie & Laura Moy, *America Under Watch* (2019), https://www.americaunderwatch.com/.

[10] Paul Mozer, *One Month, 500,000 Face Scans: How China is Using A.I to Profile a Minority*, N.Y. TIMES (April 14, 2019) https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Paul Mozer, *Inside China's Dystopian Dreams, A.I. Shame and Lots of Camera*s, N.Y. TIMES (July 8, 2018) ("China has an estimated 200 million surveillance cameras.") https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html; *Chinese Man Caught by Facial Recognition at Pop Concert*, BBC News (April 13, 2018) https://www.bbc.com/news/world-asia-china-43751276

[11] Thomas Germain, *How a Photo's Hidden 'Exif' Data Exposes Your Personal Information*, CONSUMER REPORTS, (Feb. 26, 2019) https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/

2. Investigative Face Recognition

Investigative targeting using face recognition differs from generalized face surveillance because police have some level of suspicion about a particular person. Police might have an image from a crime scene (surveillance tape, witness' iPhone video) or they might have a suspect's photograph and wish to match it with different image datasets.[12] Police are not just passively monitoring, but actively investigating a crime. Again, no federal law exists regulating the use of this technology.

As a general matter, four forms of surveillance technologies exist in this category: (a) scanning stored video footage to identify a targeted face; (b) scanning real-time video feeds to identify a targeted face; (c) scanning image databases from third-party platforms to identify a targeted face; and (4) scanning image databases from government-controlled image databases to identify a targeted face.

a. Face Recognition: Stored Footage Scans: After a crime, police may wish to run a face image they possess against stored video surveillance from a network of city cameras. The same matching technology can be used to search months of stored surveillance footage, networks of video feeds, or growing image databases to compare those images with the target's face. For example, searching stored video footage from a network of cameras could reveal the location of the person over time, including time, date, place, and patterns of movement. Depending on the density of cameras, all public movements of the targeted face could be identified and mapped. In addition, because other identifying data about the locations exist, the facial recognition matches could reveal the target's interests, employment, religious preferences, health issues, or legal troubles. Over time, a mosaic of a person's activities would be revealed by the location of the face identified by face recognition.

b. Face Recognition: Real Time Scans: Networked systems also create the potential to identify suspects in real-time. A networked system of real-time face recognition would be able to provide the specific location of a "wanted" suspect. The "hit" or "match" would alert police to the location of a particular person at a particular time in the city. Of course, in order to be able to identify that one person, surveillance cameras with the ability to match other faces would also be required to be in effect. This same type of matching would also work with single (non-networked) cameras. A single camera or drone with camera could identify a particular person in a particular place based on a face recognition match from a pre-populated dataset.

c. Face Recognition: Private Third-Party Image Scans: Private third-party providers hold massive numbers of face images, all searchable with similar technology. Police access to this dataset (via request, subpoena, or purchase) can identify suspects, groups, and associates. Photos not only provide images and identification, but also locational data from metadata which can reveal where and when the photos were taken. While not as structured, the same type of long-

[12] Jon Schuppe, *How facial recognition became a routine policing tool in America***,** NBC NEWS (May 11, 2019) https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251**;** Drew Harwell, *Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?* WASHINGTON POST (April 30, 2019) https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/?noredirect=on&utm_term=.10b8818b5bea)

term, aggregated locational information would be revealed in the collected metadata and inferences derived from the photographs.

d. Face Recognition: Identification through Government-Controlled Image Databases: Most commonly, police may wish to match a target's face image with a database of other face images in their possession. These databases could be drivers' license photos (state DMV records) or mugshot arrest photos (police-generated photos) or other more informal suspect identification systems (gang databases, jail photographs, intelligence-driven prosecution wikis). In this scenario, police have an identified suspect and want to confirm the identity of the suspect through existing photo datasets. The match might be during an investigation or even during a police traffic stop. Especially in a situation involving a suspect unwilling or unable to provide identification, the ability to quickly identify someone by their photo would be useful.

3. Non-Law Enforcement Purposes

Police may wish to use face recognition matching for non-law enforcement purposes. In some cases, the public safety interest runs to identifying victims of crime or lost children. In other cases, the technology might be used for emergency or natural disaster situations where police officials are not focused on ordinary law enforcement investigation. The limitations here involve the non-law enforcement purpose for which the face surveillance or face recognition technology is used.

These non-law enforcement uses seemingly avoid some of the problems of general face surveillance or investigatory face recognition, but, in fact, raise equally complicated questions. No matter who collects the images or who matches or for what purpose, the systems are being created to allow massive scans of large portions of the population. As a simple point, to find the lost child in the city, the surveillance system needs to be able to identify humans, children, boys, girls, race, face type, and then match the target face to all the others. This mass surveillance capability also exists if the dataset involves Facebook's billions of images as opposed to government generated images. Once society builds the architecture of surveillance that supports non-law enforcement use, they have by necessity also created the capabilities for police use.

C. Fourth Amendment Law: Recent Fourth Amendment Cases

The Fourth Amendment has little to say directly about the digital or human recognition of faces. That said, concern about arbitrary government power, systems of social control, and invasions of personal security can claim a long lineage to Founding principles.[13] While the Supreme Court

[13] In *Riley v. California*, the case that required police to obtain a warrant for a smartphone even incident to arrest, the Court offered a version of the Framer's intent:

> Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance."

does not agree on much, the Justices do agree that the Fourth Amendment was meant to limit arbitrary government powers.[14]

Facial recognition systems deployed broadly raises the specter of arbitrary surveillance. Without appropriate safeguards, face surveillance can become a generalized dragnet where every person becomes the target of government monitoring. The open question is whether the Fourth Amendment will be interpreted to be one of those safeguards.

Under a traditional Fourth Amendment analysis, a court would ask whether the technology at issue violates a reasonable expectation of privacy. This constitutional standard comes from the Supreme Court's interpretation of the Fourth Amendment in *Katz v. United States*.[15] If the technology violates a reasonable expectation of privacy, the government action would be a "search" and without a warrant or exception to the warrant requirement the search would be deemed unconstitutional. The facts of *Katz* also involved new technology, although in 1967 that new technology was a wiretap of a public free-standing telephone booth. The Supreme Court held that the electronic interception of Charlie Katz's conversation violated a reasonable expectation of privacy and thus the Fourth Amendment.[16] Notably, this development spurred Congress to pass the Wiretap Act to regulate government use of new surveillance technology involving communications. This connection has not been lost on Supreme Court Justices who have relied on this parallel to encourage congressional action on other new surveillance innovations.[17]

Under a pre-digital, traditional Fourth Amendment analysis, human observation of a face or manual photo matching would not violate a reasonable expectation of privacy. In 1973, the Supreme Court stated: "Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, *any more than he can reasonably expect that his face will be a mystery to the world*."[18] This understanding has largely continued in the context of human observation of human faces. As a result, one way of looking at existing Fourth Amendment doctrine would be to claim that it offers little protection of faces in public, no protection from photographic collection of faces, and no protection from subsequent searches of those face images.

Riley, 134 S. Ct. at 2494 (quoting 10 Works of John Adams 247–248 (C. Adams ed. 1856). According to Adams, Otis's speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." *Id.*, at 248 (quoted in *Boyd v. United States*, 116 U.S. 616, 625 (1886)).

[14] *See e.g.*, *Fla. v. Riley*, 488 U.S. 445, 462 (1989) ("The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."); *I.N.S. v. Delgado*, 466 U.S. 210, 215 (1984) ("The Fourth Amendment does not proscribe all contact between the police and citizens, but is designed "to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals.").

[15] *See Katz v. United States*, 389 U.S. 347 (1967).

[16] *See Katz*, 389 U.S. at 360 (Harlan, J., concurring).

[17] *Jones*, 565 U.S. at 427–28 (Alito, J. concurring) ("On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz*, Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U.S.C. §§ 2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.").

[18] *US v. Dionisio* , 410 US 1 (1973) (emphasis added).

Such a traditional understanding about "a reasonable expectation of privacy," however, has undergone some rethinking in recent years as the Supreme Court has begun addressing the threat of new digital technologies. Legal commentators have recognized that when it comes to new digital surveillance technologies "digital is different" for Fourth Amendment purposes.[19]

To understand how the Supreme Court might resolve the puzzle of facial recognition, it is useful to study three recent Supreme Court decisions on new technologies.[20] These privacy-protective cases help frame the analysis because they recognize the privacy and liberty threat from technology-enhanced police surveillance as distinct from traditional police surveillance.

Jones: First, in *United States v. Jones*, the majority of the Supreme Court held that placing a GPS tracking device on a suspect's car was a search for Fourth Amendment purposes because the physical act of attaching the tracking device with the intent to gain information was a "trespass" which violated the constitutional rights of the driver.[21] More importantly for our analytical purposes, five justices concurred in the outcome, reasoning that the long-term (28 days) GPS location tracking of the car in public for a drug-related crime violated a reasonable expectation of privacy and thus was a "search" for Fourth Amendment purposes.[22] These concurring justices were concerned with the privacies revealed by long term tracking in terms of habits, interests, associations, and the freedom to move without government monitoring.[23] In two overlapping concurring opinions, the Supreme Court drew a line at the government's ability to monitor individuals in public for weeks at a time. This understanding about locational privacy was reaffirmed in *Carpenter v. United States*.[24]

Carpenter: In *Carpenter v. United States*, the Supreme Court held that police typically need a probable cause warrant to acquire digital cell-site location records (CSLI) held by third party cell phone service providers.[25] Timothy Carpenter was suspected of robbing a series of electronics stores and police sought access to his cell phone location data to tie him to the crimes.[26] Using a court order authorized under the Stored Communication Act, police obtained seven days of his cell site data. This information provided police with a map of his whereabouts that corresponded with his presence at the crimes. Carpenter filed a motion to suppress the third-party records, arguing that their acquisition was a search under the Fourth Amendment and unconstitutional

---

[19] Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 951 (2016) ("So, while *Riley* perhaps left things unanswered that it could have addressed, it made very clear that when it comes to the Fourth Amendment, digital is different."); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 27 (2015); *see also* Jennifer Granick, *SCOTUS & Cell Phone Searches: Digital Is Different*, JUSTSECURITY (June 25, 2014), https://www.justsecurity.org/12219/scotus-cell-phone-searches-digital [http://perma.cc/94RH-42EV].

[20] Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 216 (2018); Margaret Hu, *Cybersurveillance Intrusions and an Evolving Katz Privacy Test*, 55 AM. CRIM. L. REV. 127, 132 (2018)

[21] *See Jones*, 132 S. Ct. at 949–52.

[22] *See id.* at 955–56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring). Chief Justice Roberts in *Carpenter* confirmed this consensus positively referencing the five justices who accepted the reasonable expectation of privacy protection of *Jones'* GPS data. *Carpenter*, 138 S. Ct. at 2215, 2217 (2018).

[23] *Id*.

[24] *Carpenter*, 138 S. Ct. at 2217 ("A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements.") (citing *Jones*).

[25] *Id.* at 2221 ("Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records.")

[26] Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL RTS. J. 495, 497 (2017).

without a probable cause warrant. The Supreme Court agreed with Carpenter holding that the acquisition of the data without a probable cause warrant violated a reasonable expectation of privacy. Chief Justice Roberts summarized the holding stating, "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[27] The focus on "depth," "breadth," scope and scale makes it clear that the Court is concerned with systems of digital surveillance.[28] The reasoning again turned on the voluminous and personal nature of the locational data being sought by police without a warrant.

Riley: Finally, in *Riley v. California*, the Court held that police must obtain a warrant before searching a suspect's smartphone incident to arrest.[29] The Court reasoned that sensitive data[30] in modern smartphones revealed too many of the "privacies of life" not to require a probable cause warrant before acquiring the information.[31] In *Riley*, the Court emphasized the quantitative and qualitative realities of digital evidence as different enough to warrant a different Fourth Amendment approach.[32] The quantitative difference involves the "immense storage capacity" which can in a very small space collect and maintain an almost infinite amount of personal data.[33] In addition, the nature and scope of digital information reveals much more qualitative information than citizens normally share with anyone else.[34]

These three cases signify the emergence of a digitally-aware Fourth Amendment, and a Supreme Court cognizant of the limitations of applying analog precedent to a digital reality.[35] Such a digitally aware Fourth Amendment would, of course, apply to the problem of facial recognition surveillance and any constitutional challenges to proposed legislation.

For purposes of this testimony, I want to emphasis two clear conclusions from these recent cases, and one less clear, but equally important, analytical framework to assess future legislation.

Digital is Different: First, the Supreme Court has made clear that precedent arising from an analog past may not control the digital future. In *Carpenter*, Chief Justice Roberts acknowledged that "a mechanical interpretation" of the third-party doctrine failed to account for the type of digital information now being collected by police through third parties.[36] He said the

---

[27] *Carpenter*, 138 S. Ct. at 2223.

[28] Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. (forthcoming 2019), https://osf.io/preprints/lawarxiv/bsedj [https://perma.cc/2EFF-UGJ3].

[29] 134 S. Ct. 2473, 2480 (2014).

[30] *See e.g.*, Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133 (2015).

[31] *Riley*, 134 S. Ct. at 2495 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[32] *Id.* at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

[33] *Id.* at 2489 ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity. … Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so.").

[34] *Id.*

[35] Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 7 (2018) ("*Carpenter* provided a rare glimmer of hope for those who wish to see a Fourth Amendment that fully grapples with the breadth and depth of technological change ....").

[36] *Carpenter*, 138 S. Ct. at 2219.

same thing in *Riley* when comparing digital smart objects recovered incident to arrest and traditional physical objects.[37] Justice Alito also recognized this truth in *Jones* when discussing the ease technology offered to track automobiles in ways that would simply be impossibly difficult with just human power.[38] Thus, the first conclusion is that the Supreme Court's willingness to distinguish analog precedent from their digital equivalents means that any legislation governing new digital surveillance (including face surveillance or face recognition) could be challenged in court and looked at with a skeptical eye by the Court.[39] In short, a mechanical reliance on analog police investigative analogies may no longer control the future. Just because police could do something without digital technology, does not mean they can do the same thing with more powerful digital technology.

Probable Cause Floor: Second, the *Carpenter* opinion provides guidance about how Congress should draft legislation around face surveillance and face recognition. At issue in *Carpenter* was a court order under the Stored Communication Act for third party records held by cell phone providers. Law enforcement agents had followed federal law to obtain the cell-site records via court order,[40] but the Supreme Court held that a higher probable cause warrant standard was required to pass Fourth Amendment scrutiny. The take away is that for some forms of facial recognition technology, a probable cause standard may be necessary to pass constitutional scrutiny. Details of the type of facial recognition requiring probable cause or a higher standard is discussed in the next section.

Future-Proofing Concerns: The third conclusion emerges from my interpretation of the recent cases.[41] But it involves *the* central issue for legislators trying to figure out whether a law allowing any face surveillance or face recognition will survive Fourth Amendment scrutiny: namely, when does the use of face surveillance or face recognition cross the line into a Fourth Amendment search requiring at least probable cause.

Admittedly, the answer is uncertain and until the Supreme Court decides a face surveillance or face recognition case we likely will not have a definitive answer. However, several themes have emerged from the recent Supreme Court decisions which provide a framework for how a court would examine the issue, and thus how Congress might think about regulating the issue.

---

[37] *Riley*, 134 S.Ct., at 2485 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered [in prior precedents]."); s*ee also Carpenter*, 138 S. Ct. at 2214 ("[W]e rejected in *Kyllo* a "mechanical interpretation" of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search.).

[38] *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring).

[39] *See, e.g.*, Orin S. Kerr, *Implementing* Carpenter, *in* The Digital Fourth Amendment (forthcoming) (manuscript), https://papers.ssrn.com/abstract_id=3301257; Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 206 (2018); Paul Ohm, *The Many Revolutions of* Carpenter, 32 Harv. J.L. & Tech. (forthcoming 2019), https://osf.io/preprints/lawarxiv/bsedj [https://perma.cc/2EFF-UGJ3].

[40] Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After Carpenter*, 128 YALE L.J. FORUM 943, 945 (2019) ("In *Carpenter*, the government had used an otherwise-valid D order to obtain Timothy Carpenter's cell-site location information (CSLI) from his cell-phone provider.").

[41] Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/ [https://perma.cc/97SL-WQNY].

I call these themes the "future-proofing" principles of the Fourth Amendment.[42] This analytical framework suggests that the Supreme Court is concerned with certain *systems* of digital surveillance technology which share a few commonalities. These principles include:

1. **An anti-tracking principle**
2. **An anti-aggregation principle**
3. **An anti-permanence principle**
4. **An anti-arbitrariness principle**
5. **An anti-pervasive surveillance principle**

The working theory is that the more a system of surveillance violates these principles the more likely it will be seen as violating a reasonable expectation of privacy and be struck down by the Supreme Court on Fourth Amendment grounds.

A brief summary of these principles follows below.

1. Anti-Tracking Principle: The Supreme Court in *Jones* and *Carpenter* was explicit in its concern about the tracking capabilities of new surveillance technologies. *Jones* was literally a case about GPS tracking and *Carpenter* a case about a network of tracking capabilities. The *Jones* Court expressed concern about the associational freedoms impacted, and the privacy revealing nature of the tracking technology:

> 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.[43]

The five concurring Justices' determination that long-term aggregated tracking was a Fourth Amendment search arose directly from the concrete harm of revealing locational data and the personal inferences derived from that information.[44] Similarly, Chief Justice Roberts in *Carpenter* recognized how the tracking capabilities of cellphones dwarfed the capabilities of GPS tracking,[45] allowing an "all-encompassing record of the holder's whereabouts"[46] and

[42] *Carpenter*, 138 S. Ct. at 2218 ("[T]he rule the Court adopts "must take account of more sophisticated systems that are already in use or in development.").
[43] *Jones*, 565 U.S. at 416 (Sotomayor, J. concurring)
[44] *Id.* (Sotomayor, J., concurring) ("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."); *Id.* at 430 (Alito J., concurring) ("Society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark.").
[45] *Carpenter*, 138 S. Ct. at 2216 ("The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.").

creating a much graver threat to personal privacy.[47] The Court has been clear that locational data should receive Fourth Amendment protection when threatened by tracking technologies.[48]

2. Anti-Aggregation Principle: Underlying *Jones* and *Carpenter* is a particular privacy harm that occurs when police can aggregate personal data. Whereas one fact revealed about a person might not invade a reasonable expectation of privacy, the long-term aggregated collection of many of those same facts will be seen as a cognizable Fourth Amendment harm.[49] Both Justice Sotomayor and Justice Alito in *Jones* separately articulated the consequences of large-scale public data collection on individual liberty. The principle was reaffirmed in *Carpenter* when the Court drew a clear line from *Jones* to the revealing nature of cell-site location data. The Court emphasized the privacy-invading nature of aggregated cell-site tracking.[50] The same theme can be observed in *Riley* with private smartphone data, when Chief Justice Roberts acknowledged how the sum of data collection can reveal more than the individual parts.[51] In a remarkable admission of the changing world, Chief Justice Roberts conceded that the aggregated information in a smartphone is probably more revealing and more privacy invading than the contents of our homes – traditionally the most protected of constitutional spaces.[52] In each of these cases, the Court found the mosaic of aggregated personal data collection a Fourth Amendment violation.

3 Anti-Permanence Principle: The anti-permanence principle involves not just collection of data but the long-term storage and retrievability of that information. The Court in both *Jones* and *Carpenter* expressed concern about the government's ability to revisit that information for any reason and for all time. This "time-machine" like capability to access permanently stored data acknowledged a fear about the creation of overbroad and unlimited data systems which allow for retrospective searching.[53] As the Court stated in *Carpenter*:

---

[46] *Id.* at 2217 ("As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations.").

[47] *Carpenter*, 138 S. Ct. at 2217-18 ("In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*.").

[48] *Id*. *See also* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH. L. REV. 189 (2015); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527 (2017)

[49] *See generally*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002).

[50] *Carpenter*, 138 S. Ct. at 2225.

[51] *Riley*, 134 S.Ct., at 2489 ("The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.").

[52] *Id.* at 2491 ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

[53] Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 939 (2016).

> Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years.[54]

This retrospective power of collected data points offers guidance about the creation of any digital system that collects personal data to be used by police for investigative purposes.

4. Anti-Arbitrariness Principle: As stated, in its recent cases, the Supreme Court has made clear its concern with the growth of arbitrary government power. In *Carpenter*, Chief Justice John Roberts stated quite simply:

> The "basic purpose of [the Fourth] Amendment," our cases have recognized, "is to safeguard the privacy and security of individuals against *arbitrary* invasions by governmental officials.[55]

This specific emphasis on arbitrariness echoed Justice Sonia Sotomayor's concurrence in *Jones* where she stated equally plainly, "the Fourth Amendment's goal [is] to curb *arbitrary* exercises of police power."[56] In both the context of cell-site locational tracking and GPS tracking the Court began with a focus on the arbitrariness of government agents gaining access to private information without a warrant. Without a constitutional or statutory check, there would be no limit on how (or against whom) police can use the surveillance technologies.

5. Anti-Pervasive Surveillance Principle: Finally, the Court in both *Carpenter* and *Jones* addressed the Fourth Amendment's foundational role in restricting police surveillance.[57] In *Carpenter* the Court stated: "a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance."[58] In *Jones*, Justice Sotomayor makes an even more direct reference to overbroad police power recognizing, "the Fourth Amendment's goal to … prevent "a too permeating police surveillance."[59] This expression of a constitutional concern with growing surveillance capacities links back to a colonial history of invasive government practices which undermined personal liberty and security and necessitated the drafting of the Fourth Amendment.

***

The clearest example of how these future-proofing principles work is *Carpenter* itself, an opinion which struck down the acquisition of seven days of third-party cell-site records because

[54] *Carpenter*, 138 S. Ct. at 2218.
[55] *Id.* at 2213.
[56] *Jones*, 565 U.S. at 416–17 (Sotomayor, J. concurring).
[57] Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse Than the Disease*, 68 S. CAL. L. REV. 1, 25 (1994) ("The warrant preference rule is a twentieth-century construction of the Fourth Amendment that is designed to restrain the discretion of police power -- a relevant concern today as it was in 1791.").
[58] *Carpenter*, 138 S. Ct. at 2214.
[59] *Jones*, 565 U.S. at 416–17 (Sotomayor, J. concurring).

it violated each of the principles. The Fourth Amendment question for facial recognition is how closely these systems mirror the same problems. The legislative question for Congress is how to regulate the technology so as to draft a law that will not be declared unconstitutional.

D. Applying Fourth Amendment Principles to Facial Recognition Technology

Applying Fourth Amendment principles to the problem of facial recognition demonstrates the need for federal legislation. While an argument can be made that the Supreme Court would strike down generalized face surveillance and require some level of probable cause for some investigatory uses of face recognition, the reality is that the Fourth Amendment "answer" is still a guessing game that will take years to clarify through constitutional litigation.

1. The Fourth Amendment & Generalized Face Surveillance

Generalized, ubiquitous face surveillance is both an anathema to Fourth Amendment principles and yet an ill fit for Fourth Amendment analysis. The problem lies in the fact that the Fourth Amendment has largely been thought to regulate police investigation, not generalized surveillance.[60] Absent special needs or special circumstances, the Supreme Court has been reluctant to allow general suspicionless searches for ordinary law enforcement purposes.[61] Applied to the problem of face surveillance, this analysis likely dooms many forms of generalized suspicionless monitoring by police.

a. Face Surveillance: Scans of Stored Footage: Face surveillance allows police to scan through stored footage providing the capabilities to track individuals by their face, aggregate their movements, interests, and patterns, and store and study these pathways for long periods of time. This type of generalized face surveillance captures everyone in its net. In terms of applying the future-proofing principles, the anti-tracking, anti-aggregation, and anti-permanence principles all apply, suggesting it would be considered the type of system of surveillance that might be a Fourth Amendment search. In addition, the surveillance would be directed against everyone in public creating a pervasive sense of police power that could be arbitrarily used or abused. This type of face surveillance system would likely be considered a search for Fourth Amendment purposes, and also would likely be considered unreasonable by the Supreme Court because of its dragnet-like quality. If the Supreme Court was concerned with tracking a single car (*Jones*) or a single cell-phone (*Carpenter*), the idea of tracking everyone without a warrant should also raise constitutional concerns. Certainly, for a system that routinely scanned everyone in public or allowed for searching stored data, the problem would raise constitutional red-flags.

b. Face Surveillance: Real-Time Scans: In the context of generalized face surveillance, real-time scans to identify individuals suffer the same Fourth Amendment infirmity. A city-wide system would flag every time an identifiable face appears on the screen. This would result in an equivalent tracking system, marking where people are located, what they are doing, and when.

[60] Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 25 (2016).
[61] Barry Friedman, UNWARRANTED: POLICING WITHOUT PERMISSION, 143-184 (2017) (explaining the difference between cause based and suspicionless searches).

While a real-time system would only provide a snapshot of presence, the data could be stored and be searchable (raising the stored footage issue). Equally importantly, the system itself "runs against everyone" and creates a similar dragnet. The future proofing principles point to a Fourth Amendment search problem, as the system can aggregate personal location data, can track individuals, and is permanent, pervasive, and arbitrary. While one might imagine the Court would allow real-time scans in certain locations, under certain circumstances generalized use for ordinary policing (especially if widely adopted) would run afoul of Fourth Amendment principles.

c. Face Surveillance: Third Party Records: Generalized use of datamining techniques to scan face images acquired from third party datasets presents a related but different problem. Again, this is a situation where the searches are without suspicion and simply for monitoring purposes. First, the fact that the images are held by third parties does not change the Fourth Amendment analysis. The Supreme Court in *Carpenter* held that the Fourth Amendment applies to government acquisition of third party records that people have a reasonable expectation of privacy over.[62] While there may be an open question about whether some images which individuals post and share deserve any Fourth Amendment protection, the scans here would go beyond public posting and include all of the hundreds of millions of photos available as well as the accompanying metadata (revealing location, time, etc.) which is not generally thought to be publicly shared. If viewed as a system of surveillance which raises concerns about the depth, breadth, and scale of personally revealing details, the resulting connections from social media images will fit the *Carpenter* rule.[63] All of the future-proofing principles also apply to generalized suspicionless face surveillance. The images will reveal a great deal of information about associational connections, location, will offer a permanent search capability, and is largely an arbitrary use of government power to monitor all (or almost all) individuals with images in these datasets. The quantity and quality of data shared is simply beyond what could ever have been found before raising similar fears to the *Riley* case.

All of these generalized face surveillance systems raise the same concerns that the Supreme Court has highlighted in their digital is different line of cases, and raise Fourth Amendment barriers to implementation. Yet, we do not know how the Supreme Court will decide the next case (should it arise), and the uncertainties about the scale, scope, and type of surveillance at issue could result in an equally unsatisfying answer.

More fundamentally, the operative limiting terms of the Fourth Amendment "probable cause" have no place in a world of generalized surveillance.[64] There can be no probable cause predicate for generalized surveillance of everyone. The lack of a limiting principle and the overbroad nature of suspicionless surveillance raise concerns with the unreasonable nature of this type of surveillance. If this type of generalized, suspicionless tracking technology using facial recognition is a search for Fourth Amendment principles, ordinary police use would likely be an unreasonable one.

---

[62] *Carpenter*, 138 S. Ct. at 2220

[63] Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. (forthcoming 2019) (manuscript), https://osf.io/preprints/lawarxiv/bsedj/ [https://perma.cc/B6HL-GS6F].

[64] Barry Friedman, UNWARRANTED: POLICING WITHOUT PERMISSION, 143-84 (2017); Barry Friedman, Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 299 (2016).

2. The Fourth Amendment & Investigative Face Recognition

Investigative face recognition presents a different analytical problem and requires a different balancing of interests. In this situation, police have a suspect's faceprint and wish to search various datasets to find a match. To be clear, the fact that police have individualized suspicion is not what changes the analysis. In *Carpenter*, *Jones*, and *Riley*, police had individualized suspicion of the suspect when they used the surveillance technology at issue. Nor is the issue who own the datasets, as the Court has found Fourth Amendment violations in both government-controlled and privately-controlled datasets.[65] Instead the inquiry is whether the surveillance system being used runs afoul of the "future-proofing" principles leading to a violation of a reasonable expectation of privacy.

a. Investigative Face Recognition: Stored Footage Scans: Face recognition scans using stored video footage might constitute a Fourth Amendment search under *Carpenter*. Like a cell-signal, a scan would reveal where a person was over time. A mosaic of geo-locational clues could be mapped to reveal a similar pattern, tracking personal details and exposing the privacies of life. Where one prays, loves, learns, and lives would all be trackable because of the identifying feature of a face. The data could be aggregated and with stored data be permanent and continually searchable. The camera system would be a pervasive surveillance power, and while targeted to the individual suspect would also capture everyone else (even if they were not identified). Again, if as has been explained, the Supreme Court is focused on the creation of a system of continuous, automatic surveillance that reveals location and personal details, a stored face recognition system seems to raise the same issues. In both *Jones* and *Carpenter*, the Court was concerned with the potential tracking capabilities more than the actual details revealed about the particular defendants. A face surveillance system provides an even more powerful potential tracking system than GPS tracking or cell-site signals.

Of course, open questions remain such as the scale of the surveillance system, the length of time in which the data is held, and whether the revealing nature of face recognition is (under the facts) really more or less revealing than a cell site signal. Unlike cell-site towers, the continuous collection of face images would depend on the density of surveillance cameras and networks. In some cities, there might be more locational details revealed than others. The Fourth Amendment question might depend on the sophistication and scale of the technology, which offers an unsatisfying constitutional answer.

b. Investigative Face Recognition: Real-Time Scans: Real-time scans that could identify whether a target is present as he/she/they pass by a face recognition enabled camera represent yet a different Fourth Amendment analysis. This situation could involve a fixed camera outside a shooting range (preventing a wanted felon from entering and possessing a gun) or a police worn body camera automatically alerting the officer to a person with an open arrest warrant.[66]

---

[65] *Carpenter v. United States*, 138 S. Ct. at 2220 ("[T]he fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection.").

[66] Ava Kofman, *Real-time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, THE INTERCEPT (Mar. 22, 2017, 2:23 PM), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/ [http://perma.cc/6Z62-ACCM]; Patrick Tucker, *Facial Recognition Coming to Police Body Cameras*, DEFENSE ONE (July 17, 2017), https://www.defenseone.com/technology/2017/07/facial-recognition-coming-police-body-cameras/139472/ [http://perma.cc/QF35-ALKU].

Separately, police could run a suspect's face image into a system and in real-time identify a current location in a city.

From one perspective, the animating concerns of the future-proofing principles are somewhat mitigated. The suspect is tracked (but to a particular location). The suspect's location is not aggregated (limited to the one identification at one location). The data is kept (but not necessarily searchable for extended periods of time). The scan is not arbitrary to the target, even if it is arbitrary when directed to those innocents captured by the camera. Under this reading, the scope of privacy invasion would be real, but limited and may not be a clear *Carpenter* violation.

From another perspective, however, the privacy harms look less benign. In order to find that one targeted suspect, a system of facial recognition identification must be in place to cull out the non-matched. Everyone is being surveilled, just not identified. Police body cameras would have the potential to scan every face. A lot of innocent people would thus arbitrarily be included in the collection which was a concern in *Carpenter*.[67] In addition, while the search is in real time, the images may still be stored and thus permanently accessible (undermining a central limitation). Finally, other people with the suspect will be collected as part of the incidental collection. The net of associational and inferential connections will grow as never before reshaping the power the government has over individuals. For this reason, the real-time targeting is less targeted than one might think and may raise constitutionally significant Fourth Amendment questions.

As a parallel, this type of investigative surveillance parallels police use of "Stingray" IMSI cellphone catchers.[68] IMSI technology allows police to find a particular cell phone out of the world of cell phone signals.[69] Using a Stingray device, a police detective could find a particular phone in a particular apartment. The Department of Justice has issued guidance requiring a probable cause warrant before using these devices.[70] Before using IMSI catchers, police must now go before a judge and obtain a warrant to target a particular phone at a particular location. The rationale is the same as it might be for a facial recognition search – in order to find the suspect's phone you need to search through all of the other signals out there, increasing the attendant privacy harms. To minimize that collection, a high standard like probable cause was adopted.

But, as may be clear, the Fourth Amendment principles do not resolve the question. The issue remains open for debate and discussion unless resolved by the Supreme Court or Congress.

c. Investigative Face Recognition: Targeted Scans of Third Party-Controlled Image Searches: The scope and scale of third-party image datasets are vast and growing, now including billions of images and videos. Police acquisition of some subset of these images to run face recognition matches for identified suspects offer a new investigatory power. If police wished to

[67] *Carpenter v. United States*, 138 S. Ct. at 2219 ("The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years.").

[68] Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J. L. & Tech. 1, 36–38 (2014).

[69] Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA Today (Aug. 24, 2015); Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, Balt. Sun (Apr. 9, 2015).

[70] DOJ. https://www.justice.gov/opa/file/767321/download.

identify a suspect by acquiring third-party face recognition images of their suspect they would be able to find more people in a fraction of the time.

Applying the future proofing principles to the problem of police acquisition of third party images for face recognition purposes is unsatisfying. On the one hand, the request for images (or the ability to search images) will reveal much more personal data than mere identity. All of the times a face is on the platform will be shown which will include information about when the photo was taken, where, and with whom. Unlike cell-site signatures, photos reveal a host of associational information because of the contextual nature of the photos (we can see the subject matter of the photo for example). While the pervasive nature of surveillance is less (or at least attributable to non-government collection), the permanence and aggregation problems remain. Tracking through the vast source of revealing personal metadata could run afoul of the *Carpenter* principles, but in truth the Fourth Amendment answer is unclear. The best that can be said is that there are interesting arguments on both sides and the Supreme Court's view on the matter is unknown.

d. Investigative Facial Recognition: Targeted Scans of Government-Controlled Image Searches: A fourth – and likely the most common type – of face recognition match will be an image match with stored government image databases. Two types of searches should be distinguished based on the type of dataset to be matched. One type of image database consists of police generated images (arrest photos, jail photos, internally generated suspect photos). Another consists of larger government image databases like driver's license photos or passport photos that include a large majority of the population.

In terms of the future proofing principles, the Supreme Court's concerns are not directly implicated. A facial recognition image match would reveal identity, but not necessarily location, tracking history, or aggregated private details. In addition, assuming there is some predicate level of suspicion (or internal police policy), the scan will not be arbitrary, and with some control over the use, the scan will not be a form of pervasive surveillance. Under existing doctrine, it is unlikely that the Supreme Court would find a Fourth Amendment violation under this analysis.

***

As is evident from the above legal analysis, the Fourth Amendment does not offer a complete or satisfying resolution to the challenge of face recognition technology. But this "failure" of the Fourth Amendment does not mean that the technology should remain unregulated. In fact, it is precisely the indeterminacy and ambiguity of the Fourth Amendment doctrine that should inspire Congress to act now and regulate.

E. Regulating Facial Recognition Technology

Legislation regulating police use of facial recognition technology must build off a constitutional floor, but need not be limited to that lower level of protection. In addition, legislation should balance the competing needs of law enforcement with the fundamental protection of individual privacy.

Even though recent Supreme Court cases do not resolve the Fourth Amendment question regarding facial recognition, three points emerge which can help shape federal legislation on the subject.

First, technology that allows arbitrary, aggregated, permanent tracking likely violates the Fourth Amendment and should be banned.

Second, analogizing to pre-digital practices no longer automatically controls the Supreme Court's decisions, and thus what was permissible for humans to do without digital assistance may not control constitutional analysis in a digital age.

Third, the Court is most worried about systems of digital surveillance and their potential privacy invading power. Together these three principles suggest a regulatory way forward on facial recognition technology.

As discussed in more detail below, Congress should: (1) draft legislation to ban the use of generalized systems of face surveillance that allow for arbitrary, aggregated, or permanent monitoring capabilities; and (2) draft legislation to prohibit the use of targeted face recognition searches absent individualized probable cause, written authorization, and minimization requirements to limit the impact on innocent citizens.

1. Congress Should Ban the Use of Generalized Face Surveillance

Federal legislation should be drafted to ban generalized face surveillance for all ordinary law enforcement purposes. Whether stored, real-time, or through third party image searches, building a system with the potential to arbitrarily scan and identify individuals without suspicion and to discover personal information about their location, interests, or activities can simply be banned by law. Separate rules can be designed for non-law enforcement purposes including public safety emergencies.

The justification for such a ban derives in large part from the Fourth Amendment principles discussed earlier. This type of suspicionless, mass surveillance system runs straight into Fourth Amendment principles, and – depending on the scope and scale – eventually could be declared unconstitutional by the Supreme Court. The combination of digital capacity, mass collection, retrospective searching, long-term aggregation, tracking, and all without any individualized or particularized suspicion should trigger significant, if not fatal Fourth Amendment scrutiny.

But the constitutional concerns extend beyond the fact that suspicionless, mass surveillance runs afoul of Fourth Amendment principles. In addition, First Amendment issues, equal application issues, accuracy, and bias concerns reinforce the need to ban face surveillance.

First Amendment Concerns: Underlying the Supreme Court's recent Fourth Amendment reasoning about privacy in public is a realization that surveillance chills First Amendment protected activity. Free expression, association, petitioning for redress, and political dissent all will be negatively impacted by face surveillance systems. Police have already shown a

willingness to use surveillance technologies to monitor dissenting voices,[71] and face surveillance will only strengthen that power. Whether protesting a government agency, or supporting an upstart political candidate challenging an incumbent, government use of face surveillance can inhibit free democratic participation and undercut political activism. In addition, individual choices to live free from government observation and participate in certain social activities, religious practices, or community groups will be curbed without a way to maintain some level of public obscurity.[72] By eroding the practical obscurity of public activity, face surveillance raises significant First Amendment issues and provides another reason to ban its use.[73]

Civil Rights Concerns: In addition to associational and expressive freedoms, face surveillance raises issues of racial justice and fairness. While surveillance technology tools, themselves, do not automatically raise fairness concerns, if past is prologue the use of the technology will impact poor communities and communities of color more than other groups.[74] The history of policing in America supports an acute awareness of the misuse of social control technologies.[75] As I have written previously in the context of the larger issues of racial bias in big data policing technologies:

> Big data's claim to objectivity and fairness must confront the racial history of American policing. Police data remains colored by explicit and implicit bias. Police data is racially coded, shaded by millions of distrustful looks and thousands of discomfiting physical encounters. The data incorporates the lived experience of African Americans, Latinos, and other people of color who have rightly or wrongly felt discriminated against because of society's suspicion. In short, big data policing must acknowledge that race is still part of modern policing. Even as code, the data is black.
>
> Acknowledging the "blackness" of police data serves two very useful goals. First, this admission pushes back against the facile claim that the issue of race can be removed by "objective," data-driven policing or that new big data technologies avoid racially biased effects. Second, the acknowledgment forces a serious examination of the very human injustices that still stir resentment and distrust in minority communities. Police can develop

[71] George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, INTERCEPT (July 24, 2015, 2:50 PM), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/; Darwin BondGraham, *Counter-Terrorism Officials Helped Track Black Lives Matter Protestors*, E. BAY EXPRESS (Apr. 15, 2015), http://www.eastbayexpress.com/oakland/counter-terrorism-officials-helped-track-black-lives-matter-protesters/Content?oid=4247605.

[72] Evan Selinger & Woodrow Hartzog, *Why You Can No Longer Get Lost in the Crowd*, NY TIMES (April 17, 2019).

[73] Woodrow Hartzog, *Body Cameras and the Path to Redeem Privacy Law*, 96 N.C. L. REV. 1257, 1259 (2018); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 388 (2013); Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way To Think About Your Data Than 'Privacy,'* ATLANTIC (Jan. 17, 2013), http:// http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283 [https://perma.cc/FA9K-B2TQ].

[74] Alvaro M. Bedoya, *The Color of Surveillance*, SLATE (Jan. 18, 2016), http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html; Dorothy Roberts & Jeffrey Vagle, *Racial Surveillance Has a Long History*, Hill (Jan. 4, 2016), http://thehill.com/opinion/op-ed/264710-racial-surveillance-has-a-long-history.

[75] *See* Alex Vitale, THE END OF POLICING (2017); Paul Butler, CHOKEHOLD: POLICING BLACK MEN, 59–61 (2017); Angela Davis, POLICING THE BLACK MAN: ARREST, PROSECUTION, AND IMPRISONMENT, 178–233 (Angela J. Davis ed., 2017).

technologies to address and overcome these racial tensions, but first the adopters of data-driven systems must acknowledge and design around this racial reality.[76]

There is little reason to think that the development of face surveillance technology will be different than past uses of surveillance technology. Early adopters have targeted poor urban areas and communities of color.[77] The choices of where the cameras are placed, which datasets are used, how they are used, and who is targeted must be interrogated in order to avoid implicit or explicit discriminatory uses. Because of this history, and because of the danger of using facial recognition technologies to surveil poor communities and communities of color, the argument to ban this type of use grows stronger.

Accuracy & Bias: Finally, face surveillance does not always work as intended. Real concerns have been demonstrated about the accuracy of face surveillance matches.[78] The danger of false positive hits is real and the consequence for such a false match means a coercive and potentially dangerous encounter with police. In the context of face surveillance with tens of thousands of faces being scanned every day, the reality of inaccurate matching technology will create significant practical problems. These inaccuracy concerns combine with bias concerns as current facial recognition has shown a higher error rate with people of color.[79] A policing technology that combines inaccuracy, racial bias, and the possibility of deadly police force is dangerous.

In sum, generalized face surveillance should be banned under federal law, with the only exceptions being for emergency or non-law enforcement uses.

2. Congress Should Require a Probable Cause-Plus Standard (akin to the Wiretap Act) for Investigative Face Recognition

Federal legislation should authorize use of face recognition for investigative targeting on a probable cause-plus standard, requiring an assertion of probable cause in a sworn affidavit, plus declarations that care was taken to minimize unintended collection of other face images, and that proper steps have been taken to document and memorialize the collection.[80] This standard would apply to all face recognition, including stored surveillance scans, real-time scans, third party image scans, and even government-collected image scans. As will be discussed below, this rule fills the gaps of Fourth Amendment protection, and also responds to the different ways digital surveillance technologies will expand in scope and scale over time.

Probable Cause-Plus Standard: As an initial matter, Congress should recognize that a model for this type of probable cause-plus framework for surveillance oversight already exists in the form of the Wiretap Act.[81] Designed to address another form of valuable, but personally

[76] Andrew Guthrie Ferguson, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT, 131-32 (2017).
[77] Clare Garvie & Laura Moy, *America Under Watch* (May 2019), https://www.americaunderwatch.com/.
[78] Clare Garvie, *Flawed Face Data* (May 2019) https://www.flawedfacedata.com/.
[79] Joy Buolamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, TIME (Feb. 7. 2019), http://time.com/5520558/artificial-intelligence-racial-gender-bias/; Clare Garvie & Jonathan Frankle, *Facial Recognition Software Might Have a Racial Bias Problem*, Atlantic (Apr. 7, 2016).
[80] David Gray, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE, 255-57 (2017).
[81] Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 14 (2004) (describing the history of the Wiretap Act and how it can be adapted to new technologies); *see also* Laura K. Donohue, *Technological Leap,*

revealing information, the Wiretap Act provides access to personal communications on a showing of probable cause plus a few other limitations.[82]

In simplified form, the requirements of the Wiretap Act are four-fold: (1) probable cause that a crime has been committed, (2) a minimization requirement to avoid unnecessary collection, (3) a declaration that other means of investigation have been exhausted, and (4) a particularized statement about the length of time and type of communication sought. Notably, this process has been used without significant complaint for decades by investigators and the courts in the context of communications.

In the facial recognition context, a parallel process would be even easier because all that would be required is a showing of probable cause that a crime had been committed, a declaration that the face recognition search was necessary because there were no other ways to obtain an identification, a statement about how other images of innocent people would be minimized, and the reason why police thought the target's image would be in the particular dataset. Like the Wiretap Act, this process could be formalized and standardized.

For some forms of targeted face recognition (stored footage scans, third-party images scans with metadata), this type of probable cause-plus standard is not only preferable, but likely constitutionally necessary to survive a Fourth Amendment challenge. If the Supreme Court is going to require probable cause for systems of government surveillance that can reveal location, patterns, interests, and identity, some forms of facial recognition matching should be regulated by an appropriately high constitutional standard (probable cause or probable cause-plus).

But, even if not constitutionally required, in the other face recognition use cases, Congress would be wise to future-proof its legislation with this heightened probable cause-plus standard for face recognition scans through real-time footage and government-controlled image databases. The main reason for this requirement involves the same "digital is different" fears articulated by the Supreme Court, namely that the quantitatively and qualitatively different capabilities of digital matching requires caution and greater court oversight.

The argument here is two-fold: first, because of the growing scale of digital images and the ease of automating face recognition a heightened legal standard and additional legal process should be

---

Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age, 97 MINN. L. REV. 407, 491 (2012); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 2 (2007); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1280 (2004).

[82] 18 USC § 2518 reads in relevant part:

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--
(a) the identity of the person, if known, whose communications are to be intercepted;
(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and
(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

18 U.S.C.A. § 2518(4) (West 2019)

legislatively required. Second, this probable cause-plus standard will be relatively easy to meet in the face recognition context.

Scale and Automation: The scale of digital images available to police is simply too great to allow unregulated face recognition scans. Whereas today a police officer might just match a target's face to a local jail database that police control, the ability tomorrow to search any other database of images needs to be regulated. Even the FBI's own image database has grown to now include access to a network of more than 400 million images.[83] The simple fact is that any government-controlled database can be expanded to include any number of images bought, scraped from the web, or developed organically.

In addition, the ease brought on by automation makes these searches something different in kind than traditional photo matches. It would be a mistake to mechanically equate past human search practices with the quantitatively and qualitative different capabilities of artificial intelligence powered pattern matching systems. Just because a police officer once could match a target image with a paper mugshot book does not mean that the same officer should be able to run that image against 400 million images (or billions of Internet images) without any cause. Too many innocent people are caught in that web[84] and the capacity is simply too powerful without regulation.[85]

Finally, the requirement of probable cause-plus will prevent warrantless face recognition from becoming an automated and continuous process. If police need no cause or justification to run a search of an image against their growing image datasets, they could also automate this process. The result would be that every photograph in police possession, or every photo taken through police body cameras could be uploaded to see if a face recognition match occurs (with all the images permanently stored for future searches). A probable cause-plus requirement, while not mandated by the current Fourth Amendment doctrine, allows for a balance of interests akin to Wiretap Act. With a warrant, police can search a system for a real-time match, but they cannot automatically program the system to provide an alert on all real time matches. In addition, they would be required to take steps to minimize unwanted collection and unneeded images.

Application: The requirement of probable cause-plus will not be burdensome to meet in the context of face recognition. In many cases police have probable cause of a crime and a suspect's photo. They wish to run the image in a particular database because they have no other leads. They have a defined purpose, a defined image dataset, and probable cause to believe that the face they are searching for will be in the dataset. If all of these things are true, they would meet the requirements of a probable cause-plus warrant under a Wiretap Act-like process.[86]

---

[83] GAO Report, https://www.gao.gov/assets/680/677098.pdf

[84] Kaveh Waddell, *Half of American Adults Are in Police Facial-Recognition Databases*, THE ATLANTIC (Oct. 19, 2016) https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/.

[85] Evan Selinger & Woodrow Hartzog, *Amazon Needs to Stop Providing Facial Recognition Tech for the Government*, MEDIUM (June 21, 2018).

[86] Such a process has been proposed for other new digital technologies. *See* Natalie Ram et al., *Genealogy Databases and the Future of Criminal Investigation*, 360 Science 1078 (2018) (discussing a Wiretap Act like requirement for genetic databases); David Gray, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE, 255-57 (2017) (proposing a Wiretap Act like process for tracking technologies); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 497 (2012) (discussing a Wiretap Act like process for biometrics).

As an added benefit, the process will generate a written record allowing for a measure of transparency, accountability, and the avoidance of abuse. Probable cause warrants are not simply about justifying an intrusion into personal privacy, but also about documenting the use after the fact. Written records will reveal the scale, scope, and efficacy of the programs and also allow regular auditing and accountability. Stories have already begun to emerge about the consequences of an unregulated system of face recognition.[87] Finally, the warrant process will provide a record to study if any alterations were made to the searched photos or any deviations made in the process of obtaining a match, and also create a formal record suitable to be provided to prosecutors and defense counsel consistent with due process protections.

F. Conclusion

Congress should ban face surveillance and restrict face recognition technology before widespread national adoption by law enforcement.[88] While the Fourth Amendment offers insights on how to think about the growing threats of systems of surveillance, constitutional law is slow to protect personal privacy and individual liberty in the face of rapidly accelerating technologies of social control. As Justice Alito has written, "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."[89]

[87] Drew Harwell, *Police Have Used Celebrity Look-alikes, Distorted Images to Boost Facial-Recognition Results, Research Finds*, WASH. POST (May 16, 2019).
[88] This testimony focuses on the specific problem of government use of face surveillance and face recognition and not private use of the technology. Additional legislation may be required for the problem of private use.
[89] *United States v. Jones*, 565 U.S. 400, 429–30 (2012) (Alito, J. concurring).

Biographical Summary

Professor Andrew Guthrie Ferguson is a national expert on predictive policing, big data policing, and emerging surveillance technologies. He is the author of the book THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017). His recent research focuses on studying how new law enforcement technologies distort traditional methods of policing and the related issues of privacy, civil rights, and community safety. He is a Senior Visiting Fellow at the Harvard Law School Criminal Justice Project and a Technology Fellow at the NYU Law School's Policing Project.

Professor Ferguson teaches as a tenured full professor at the University of the District of Columbia's David A. Clarke School of Law. His scholarship on the digital transformation of criminal justice has been published in the *University of Pennsylvania Law Review*, the *California Law Review*, the *Cornell Law Review*, the *Minnesota Law Review*, the *Northwestern Law Review*, the *Boston University Law Review*, the *University of Southern California Law Review*, the *Notre Dame Law Review*, and the *Emory Law Journal* among others. In 2017 Professor Ferguson co-authored the law professors' amicus brief to the Supreme Court on behalf of the Petitioner in *Carpenter v. U.S.*, involving the warrantless collection of cell-site tracking data.

Professor Ferguson's legal commentary has been featured in numerous media outlets, including *The New York Times*, *The Washington Post*, *The Economist*, CNN, NPR, USA Today, the ABA Journal, *The Atlantic*, and many other national and international newspapers, magazines, and media sites. He is regularly consulted by governments, private industry, local community groups, and civil liberties organizations interested in the future of policing.

Professor Ferguson holds an LL.M from Georgetown Law Center, a J.D. from the University of Pennsylvania School of Law (*summa cum laude*), and a B.A. from Williams College (*cum laude*).