2021

The Fourth Amendment's Transformation in the Modern Age and Effects on Facial Recognition Service Providers

Brendan Bianchi

Introduction

The use of facial recognition technology (FR) by public and private actors has stirred controversy in recent months. There is a myriad of uses of facial recognition, some more ominous than others. Apple uses FR to map the contours of a user's face to restrict access to the user's phone.[1] Coffee shops may incorporate facial recognition software into coffee makers to pour a cup of coffee for a yawning passerby.[2] Consternation over FR arises more often, however, when the technology is used in less anodyne ways. Law enforcement's use of FR has sparked outrage among civil liberty activist groups, resulting in litigation over possible privacy infringements.[3] Facial recognition service providers (FRSP's) and tech investors watch these lawsuits carefully to gauge where courts are drawing the boundaries by which FR use by the government is legally permissible. But to understand the legality of government use of FR, we first have to understand how it is frequently developed and applied.

Law enforcement has increasingly hired facial recognition service providers to code software capable of "scraping" images off the Web. Web scraping is simply a term used to describe various methods used to extract data from websites. These images are scraped from images posted on third party platforms, including Facebook, LinkedIn, Twitter, etc.[4] Subsequently, these images are shifted and stored into the software's database.

---

[1] Maggie Tillman, *What is Apple Face ID and how does it work*?, Sep. 18, 2019, POCKET-LINT.COM, https://www.pocket-lint.com/phones/news/apple/142207-what-is-apple-face-id-and-how-does-it-work.
[2] Ron Dicker, *Machine Dispenses Free Coffee When You Yawn*, July 19, 2013, HUFFINGTON POST, https://www.huffpost.com/entry/coffee-machine-yawn_n_3623787.
[3] Drew Harwell, *ACLU sues FBI, DOJ over facial recognition technology criticizing unprecedented surveillance secrecy*, Oct. 31, 2019, WASHINGTON POST, https://www.washingtonpost.com/technology/2019/10/31/aclu-sues-fbi-doj-over-facial-recognition-technology-criticizing-unprecedented-surveillance-secrecy/.
[4] Shivdeep Dhaliwal, *Facebook Sends Cease And Desist Letter To AI Startup, Joins Twitter, Venmo, YouTube*, Feb. 6, 2020, YAHOO FINANCE, https://finance.yahoo.com/news/facebook-sends-cease-desist-letter-111645892.html.

Government interest in FR surged following the terrorist attacks on 9/11.[5] Following the Cold War, the United States did not have a major military hegemony to compete with. Instead, the emerging enemy was "asymmetric threats" or, in other words, unidentifiable enemies targeting "soft targets," like malls and airports.[6] Asymmetric threats do not play by conventional rules of war. The United States realized it was going to be forced to employ unorthodox, legally suspect ways to combat asymmetric threats. Around this timeframe, the United States was excelling in technological development. The government viewed FR as an opportunity use its strengths in its fight against these new threats. Biometrics industries sprung out of this time period.[7] As innovation spurred, robust FR systems were developed. To date, the system nearest to being able to identify faces in a crowd using real-time surveillance is the Biometric Optical Surveillance System (BOSS).[8] Developed through funding from the Department of Homeland Security, BOSS is still used today. BOSS can use video cameras to scan people in public and then identify the names of individuals by cross-referencing their faces with other databases.[9]

Today law enforcement agencies can access similar databases at any time for its investigations. For example, if a convenience-store camera captures footage of a burglar breaking and entering the store, assuming the image is of high enough quality, law enforcement can use the software to match the image with one of the images in its database. Technological advancements in the fields of photography and videography, however, have facilitated better opportunities for stock images, worthy of facial recognition, to appear in image databases.[10] Matching the image

[5] Eric Z. Wynn, *Privacy in the face of surveillance: Fourth Amendment considerations for facial recognition technology,* NAVAL POSTGRADUATE SCHOOL, 19 (2015).
[6] Eric Z. Wynn, *Supra* Note 5.
[7] Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance,* 100 (2011).
[8] Eric Z. Wynn, *supra* Note 5 at 22.
[9] Ginger McCall, *The Face Scan Arrives*, THE NEW YORK TIMES, August 30, 2013, http://www.nytimes.com/2013/08/30/opinion/the-face-scan-arrives.html?_r=0.
[10] Federal Trade Commission, *FTC Recommends Best Practices for Companies That Use Facial*

does not necessarily have to be executed manually. The software can unilaterally measure the biometric landmarks of a person's face, including the nose, face, eyes, skin pores and pair those results with another image in the database to find a match. Law enforcement has used this tool to shave time usually spent on investigations from weeks to mere hours.[11]

Some argue this tool greatly enhances civil liberty and dignity by reducing the pool of suspects; thus, reducing the costs and humiliation entailed in being a suspect in a criminal investigation.[12] Facial recognition technology has the potential to greatly enhance policing and government security efficiency in the United States. The advancement of FR could potentially accomplish in seconds what would take hundreds or thousands of man-hours to complete manually. The decades-long development of FR is coming to a point where, in the near future, personal information about people can be so quickly accessed that their identity, location, and other personal information can be determined and logged within seconds. This technology, if left unregulated by law, should be particularly troubling to those who have no reason to be concerned with law enforcement surveillance. Richard Posner, an American jurist, argues that when privacy values are compared to security from terror-related deaths often associated with asymmetric tactics, privacy should lose to security.[13] Posner goes even further in a later writing, arguing that individuals often use privacy law as a cover for the disreputable parts of our character.[14] Posner, like many others, share the view that privacy rights are overvalued and diminish very little

Recognition Technologies, October 22, 2012, http://www.ftc.gov/news-events/press-releases/2012/10/ftcrecommends-best-practices-companies-use-facial-recognition.

[11] Lee Kicker, *How Criminal Investigations Can Be Expedited Using Facial* Recognition, May 7, 2018, NEC Corporation of America, https://nectoday.com/how-criminal-investigations-can-be-expedited-using-facial-recognition/#.

[12] Amitai Etzioni, *Facial Recognition Meets the Fourth Amendment Test*, Sep. 22, 2019, THE NATIONAL INTEREST, https://nationalinterest.org/feature/facial-recognition-meets-fourth-amendment-test-82311.

[13] Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (New York: Oxford University Press, 80 (2006).

[14] See Richard A. Posner, *Privacy, Surveillance, and Law*, 75 UNIVERSITY OF CHICAGO LAW REVIEW 245 (2008).

freedom. However, the slippery-slope concerns that privacy advocates have about the FR's potential for extensive abuse may not be completely without merit, as we will see.

FR certainly has its public benefits. But it is also a tool that can be easily abused if placed in the wrong hands. China has employed a vast network surveillance system using FR to monitor and rank people based on their behaviors. This so-called "social credit system" imposes rewards and punishments on individuals based on the scores they receive. For example, behaviors like jaywalking and buying videogames have been deemed punishment-worthy behaviors that, if caught red-handed by the network, can lead to lower social credit. Some of the punishments for low social credit include restrictions on travel, employment opportunities, and school choice.[15]

China presents an example of the draconian use of FR, but the use of the technology in the United States has not been nearly as eerie. Many police departments have made clear that they do not engage in mass data gathering (e.g., placing cameras on street corners). Instead most police departments are transparent about their use of FR to local communities to convey an image of responsibility, professionalism, and to avoid media backlash.[16] Clearview AI, a FRSP, has professed to only scraping publicly available images off social media sites.[17] Compared to China's social credit system, these uses are anodyne; however, concern about the ethics of FR gathering and application are growing among members of the private sector. Axon, a major police body camera manufacturer, has rejected selling FR, citing the findings of an independent ethics panel

[15] Alexandra Ma, *China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish* you, Oct. 29, 2018, BUSINESS INSIDER, https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4#5-keeping-you-out-of-the-best-hotels-5.

[16] Associated Press, *ACLU calls out Amazon, Washington Co. sheriff's office for facial recognition* tech, May 22, 2018, KGW8, https://www.kgw.com/article/money/aclu-calls-out-amazon-washington-co-sheriffs-office-for-facial-recognition-tech/283-557099068.

[17] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, Jan. 18, 2020, The New York Times, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

which found FR to not be advanced enough for law enforcement to depend on.[18] Microsoft recently announced its refusal to continue investing in AnyVision, a FRSP, due to oversight concerns.[19] Facebook and Twitter have sent cease-and-desist letters to Clearview AI, demanding it stop scraping images off their websites in violation of their terms-of-service.[20]

Government crackdowns on FR have moved at warp speed. Legislators in San Francisco have already imposed an outright ban on government use of FR. But that's not all. Additionally, any new plans to purchase FR must now be approved by city administrators. These measures are deemed drastic by some, especially among members of the law enforcement community. Some believe that a moratorium is more appropriate, as opposed to an outright ban. Experts believe that as the technology develops, ways to limit FR to responsible use will bloom. Senators Jeff Merkley (Oregon) and Cory Booker (New Jersey) have proposed a bill that would do just that. The bill, proposed in February, calls for a moratorium on using the technology until a commission recommends guidelines and limitations for government use.[21] The bill does not restrict private purchases of FR.

Federal consumer privacy laws are generally ineffective at hampering abuse of an individual's personal information. There are a few reasons for this. For one, privacy law in the United States operates across subject matters (e.g., COPPA for children, HIPAA for health services, etc.) There is no blanket statutory regime governing consumer privacy. Second, consumer information has been protected by a self-regulatory regime articulated by the Federal Trade Commission (FTC). This model, known as "notice and choice," encourages firms to adopt

[18] First Report of the Axon AI & Policing Technology Ethics Board: pg. 28-30 (June, 2019).
[19] Nick Statt, *Microsoft to end investments in facial recognition firms after AnyVision controversy*, Mar. 27, 2020, THE VERGE, https://www.theverge.com/2020/3/27/21197577/microsoft-facial-recognition-investing-divest-anyvision-controversy.
[20] Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, Jan. 22, 2020, THE NEW YORK TIMES, https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html.
[21] Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (2019-2020).

substantive information protections via "privacy by design" and disclosure of its data collection practices to consumers. The notice-and-choice model was extended into the FTC's best practices guideline for facial recognition, including a policy directing that digital signage using the technology not be set up where kids congregate.[22]

Privacy by design incorporates substantive consumer protections into the firm's practices including data security, reasonable limits on data collection, comprehensive data management procedures, and sound data retention and accuracy practices.[23] This model works as an intermediary between strict regulation and entrepreneurial freedom. Most policies, however, do not comply with FTC guidelines.[24] Although FTC threats of regulation have given firms an incentive to reign in irresponsible data collection practices, the FTC's ability to sanction for noncompliance is limited and actions brought by the FTC are frequently based on firms misrepresenting practices outlined in its privacy policy.

The Stored Communications Act of 1986 will only provide a temporary sigh of relief to privacy advocates. Companies that store and transmit user data are generally prohibited from "knowingly" sharing those records with the government.[25] But this does not put and end to the commercialization of biometric data. FRSP's are free to transmit data to other private parties such as data brokers. Data brokers are firms that buy and sell information about individuals for the purpose of aggregating the data to create individual profiles.[26] This information may range from individual pieces of information, like age or weight, to more sensitive information, like web-browsing histories, bank card transaction records, and driving records. FRSP's may even operate

[22] Federal Trade Commission: Best Practices for Common Uses of Facial Recognition Technologies, p. 2 (2012).
[23] See generally Federal Trade Commission: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, (2012).
[24] Florencia Marotta-Wurgler, *Understanding Privacy Policies: Content, Self-Regulation, and Markets*, p. 4 (2016).
[25] Stored Communications Act of 1986, 18 U.S.C § 2702 (1986).
[26] Federal Trade Commission: DATA BROKERS: A Call for Transparency and Accountability, (2014).

as a data broker operation. This would allow them to sell biometric information directly to law enforcement, assuming no other state restriction bars the transaction. Clearview AI is an example of a FRSP that operates as a data broker.

As you have seen thus far, attitudes towards facial recognition gathering methods and application are somewhat mixed in the current climate. There is a sense that lawmakers and investors are becoming increasingly queasy about the ethics of its use. But as the technology develops and effective measures to reign in corrupt practices are discovered, its potential to be used as a robust crime-fighting tool is promising. This prospect makes FR a potentially rewarding space for tech startups and investors. In fact, market reports project the facial recognition industry to grow and develop in the coming years.[27] Factors driving the market include increased technological advancements across verticals, a growing surveillance market, and rise in defense deployment. However, in light of the maelstrom of landmark global and domestic events in recent months including the impeachment of President Trump and the effects of the COVID-19 pandemic, large-scale public debate over this topic has not come to full fruition. Most Americans may even find the topic overly confusing or obscure. This leaves the FR space at the mercy of an unforeseen shift in political sentiment. Should the sentiment cut against government use of FR, FRSP's will have to discover novel and creative ways to employ the technology that comport with new laws—or abandon the project altogether.

But what happens if public sentiment remains mixed on government use of FR as a crime-fighting tool? Given the volatility of this political climate, it isn't unreasonable to assume that debate on this subject will continue to be pushed to the backburner of most political agendas. Keep in mind, most states have not passed any explicit restrictions on FR. More importantly, Illinois,

[27] MarketsandMarkets, *Facial Recognition* Market, (June, 2019), https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html.

Texas, and Washington are the only states to have passed legislation providing individuals with a private cause of action for having their biometric information collected.[28] This means in the other forty-seven (47) states, FRSP's are mostly free to engage in scraping. This poses a problem for staunch privacy advocates. In the face of a porous privacy regime and distracted state legislatures there is a severe lack of weapons in their arsenal to combat FR gathering and use. Consequently, in light of the growing prevalence of FR use in law enforcement, criminal defendants identified by FR will be on the front lines in the war against the technology using the Fourth Amendment as both sword and shield.

I. The Biometrics Industry

FRSP's operate within the biometrics industry. The mass collection of biometric information has expanded rapidly in the past decade. According to a market research report by Application, Technology, Function, & Geography, "the biometrics market is expected to reach $32.73 billion by 2022."[29] More recent forecasts have the biometric technology market surpassing $44 billion globally by 2021.[30] This could be due to the combination of spiraling use of the technology and lack of regulation the space. To put it simply, biometrics are biological measurements.[31] Any physiological or behavioral trait can be characterized as a biometric characteristic. Examples

[28] Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, Dec. 16, 2019, Wired, https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/.
[29] Biometric System Market by Authentication Type (Single-Factor: (Fingerprint, IRIS, Palm Print, Face, Vein, Signature, Voice), Multi-Factor), Component (Hardware and Software), Function (Contact and Non-Contact), Application, and Region - Global Forecast to 2022, MARKETSANDMARKETS (Nov. 2016), http://www.marketsandmarkets.com/Market-Reports/nextgeneration-biometric-technologies-market-697.html.
[30] Natasha Kohne, Isabelle Gold & Kamran Salour, *Unique Biometric Data Creates Unique Privacy Concerns*, NEW YORK LAW JOURNAL, 1 (Feb. 22, 2016). https://www.akingump.com/a/web/41212/aoi8x/070021626-akin.pdf.
[31] See Definition: Biometrics, MERRIAM-WEBSTER, https://www.merriamwebster.com/dictionary/biometrics (defining biometrics as "the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity").

include hand geometry, fingerprints, DNA, retina, iris, or ear features, and—relevant to our purposes—faceprints.[32]

The term "biometrics" is also used to describe a system. Biometric systems consist of three basic components: first, a device that captures the biometric characteristic; second, "software to convert the scanned biometric data into a standardized digital format and to compare [relevant] match points;" and third, "[a] database to securely store biometric data for comparison.[33] The biometric information is compiled in a database, which are used to create an algorithm of an individual's biometric characteristics. In the context of FR, this would include biometric nodes on one's face.[34] Once in the database, the data can be used to verify an individual or identify an unknown person using new information.[35]

The government and private businesses gather vast amounts of biometric data for a myriad of purposes. Private companies buy and sell this information to each other, and in some cases, directly to the government, creating a commercialized industry for sensitive information.[36] Readers new to this space may be new to the value such information has to innovators. Biometric characteristics provide extraordinarily unique datasets for many companies, not just law enforcement. For

---

[32] Grandview Research, *Biometrics Technology Market Analysis Report By End-Use (Government, Banking & Finance, Transport/Logistics, Defense & Security), By Application (AFIS, Iris, Non-AFIS), and Segment Forecasts, 2018 – 2025*, GRAND VIEW RESEARCH, (2018). https://www.grandviewresearch.com/industry-analysis/biometrics-industry.

[33] See Margaret Rouse, Definition: *Biometric Verification*, SEARCHSECURITY.COM, http://searchsecurity.techtarget.com/definition/biometric-verification (last updated May 2008).

[34] See *Infra* note 29.

[35] Erin M. Sales, Note, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to be Free from Self-Incrimination*, 69 U. MIAMI L. REV. 193, 213–14 (2014).

[36] Gregory James Evans, *Comment, Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 195 (2015).

example, if a patient cannot communicate their symptoms, a provider can scan the patient's voice and access his/her records to identify the illness.[37]

Businesses are using biometric data in ways the average consumer may engage with daily without recognizing. Companies may employ biometric technologies to increase efficiency and reduce fraud. Consider a modern update to the time clock for employees logging in and out of work. Biometric readers allow workers to simply tap their fingerprints onto a biometric fingerprint scanner, as opposed to punching a timecard. This can reduce a practice called "buddy-time" punching to increase workplace efficiency and accountability.[38] Many tanning salons and gyms allow members to enter and use the facility by simply using a fingerprint scanner.[39] Banks are researching ways to use biometric data to curb identity theft, and some have successfully implemented measures. Citi Bank has introduced a voice authentication system to identify the identities of customers explaining issues to customer service representatives over the phone.[40] Wells Fargo uses eye-print authentication as an added security layer for clients to view account balances, make deposits, and approve payments from mobile devices.[41] Even more interesting is Barclays's Finger Vein reader Technology. customers simply place a finger inside a small desktop scanner instead of entering passwords and PINs.[42]

Biometric technologies clearly provide a boost to consumer experience, but the commercialization of such sensitive data appears to create perverse incentives. We are now in a

[37] Definitive Healthcare, *3 Ways Biometric Technology Improves Hospital Performance*, DEFINITIVE HEALTHCARE, (Jan. 8, 2020). https://blog.definitivehc.com/ways-biometric-technology-improves-healthcare.
[38] See Dixon v Washington and Lee Smith Community-Beverly, et al., 2018 WL 2445292 (USDC IL ND, 20180531).
[39] Jason Knowles, *Finger scanning gaining in popularity, raising security concerns,* ABC 7 (Feb. 6, 2015). https://abc7chicago.com/finger-printing-fingerprints-prints-biometric-screening/507502/.
[40] Alison Arthur & Bethany Frank, *Five Examples of Biometrics in Banking,* ALACRITI (May, 8, 2019). https://www.alacriti.com/biometrics-in-banking.
[41] Alison Arthur & Bethany Frank, *Supra* Note 39.
[42] Alison Arthur & Bethany Frank, Supra Note 39.

situation where the business gathers intimate, personal information and sells it to buyers that consumers may not have wished to expose themselves to, like the government. And the United States privacy regime does not give individuals the power to protect their privacy by controlling the personal data gathered, collected, stored, and sold by the private industry.[43] This is problematic given the "private industry tracks 24/7 our physical location, online travels, friends, activities, likes and dislikes, preferences (including religious and sexual), personal status (married, divorced, or single), and financial status. Such tracking is accomplished in myriad ways and, more increasingly, it is done using individuals' biometric identifiers."[44] Later on you will see that this is a concern for Justices on the U.S. Supreme Court.[45]

The companies mentioned thus far that have employed biometric technologies are considered FRSP's for purposes of this project. These companies use biometric technology in what many may consider to be anodyne ways. However, the main concern that privacy advocates have is the sharing of this information—and not necessarily with other private companies, but with data brokers. As mentioned in the Introduction section of this project, data brokers. Recall that data brokers are firms that buy and sell information about individuals for the purpose of aggregating the data to create individual profiles.[46] Data brokers, unlike companies that typically employ FR, don't deal directly with consumers, allowing them to sell information directly to the government. Consumers may be inadvertently conveying private information to the government via private businesses that sell their biometric data to data brokers.

[43] Anne T. McKenna, Pass Parallel Privacy Standards or Privacy Perishes, 65 RUTGERS L. REV. 1041, 1042 (2013).
[44] Id. at 1043.
[45] *Infra* Note 89.
[46] Federal Trade Commission, *Supra* Note 26.

II. How Facial Recognition Technology is Used

Before traversing through the legal terrain of FR, it's important to know how the technology works in practice. Although the thought of FR seems hyper-futuristic, the technology is currently used in many ways. The technology is easy to understand when broken down step by step. This method of learning helps avoid thinking about facial recognition in an overly abstract fashion that clouds our judgment in assessing FR's position in the legal terrain.

Consumers may purchase a facial recognition camera with the technology already embedded or can reconfigure the components of the camera to function as a facial recognition camera. The latter may take considerable time and effort to execute, so most consumers simply purchase a camera with facial recognition already embedded. The camera will then capture an image of a face, alone or in a crowd.[47] FR strays from traditional surveillance in the sense that the typical camera captures naked images. FR captures and measures an individual's biometric nodes.[48] Examples of biometric nodes include the distance between the nose and eyes, the amount and type of skin pores one has, and relative position of the nose, jaws, and cheekbones.[49] Individuals will often be under the mistaken impression that the camera is operating as a traditional security layer when in fact it is collecting biometric data.[50] Many grocery stores, schools, and airports use facial recognition cameras.[51]

The analysis of a face is then turned into a mathematical formula.[52] These facial features become numbers in a code. This numerical code is called a faceprint. Similar to the unique structure of a thumbprint, each person has their own faceprint. That faceprint is then compared to

[47] Electric Frontier Foundation, *Facial Recognition*, (Oct. 24, 2017), https://www.eff.org/pages/face-recognition.
[48] Panda Security, *The Complete Guide to Facial Recognition Technology*, 2019, https://www.pandasecurity.com/mediacenter/panda-security/facial-recognition-technology/.
[49] Panda Security, *supra* note 22.
[50] Panda Security, *supra* note 22.
[51] Electric Frontier Foundation, *supra* note 21.
[52] Panda Security, *supra* note 22.

a database comprised of other faceprints and finds a match if available. Law enforcement mostly uses FR for investigatory leads because such evidence is not yet admissible in most courts.[53] The FBI has access to more than 641 million photos, including 21 state databases such as Division of Motor Vehicles (DMV).[54] There are questions as to the technology's ability to accurately identify a match. A report on the use of face recognition in the UK found that the technology led to false matches over 90 percent of the time.[55] Academic research has also already shown that face recognition is less accurate for non-white faces and women.[56] Law enforcement primarily employs FR in two scenarios: When a suspect has been detained but there is no other way to identify the suspect, or when footage of an unidentified suspect is captured.[57] Assuming the image is of sufficient quality, law enforcement will input the suspect's faceprint into the system to identify a potential match.[58]

III. The Inefficiency of Traditional Fourth Amendment Doctrine in the Context of Big Data Cybersurveillance

Applying the Fourth Amendment in the Digital Age has been a common cause for consternation among judges. Since Katz v. United States, the "reasonable expectation of privacy" standard has governed the Fourth Amendment analysis.[59] The court strayed from its original

---

[53] See People v. Collins, 15 N.Y.S.3d 564, 576 (N.Y. Sup. Ct. 2015).
[54] Neema Singh Guliani, The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database, ACLU (June 7, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through.
[55] Brendan F. Klare, et al., *Face recognition performance: Role of demographic information*, IEEE Transactions on Information Forensics and Security, p. 10-11, (2012).
[56] Brendan F. Klare, et al., *supra* note 27, at 12.; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, 1, 12 (2018).
[57] Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, July 2019, NACDL.ORG, https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/challenging-facial-recognition-software-in-criminal-court_july-2019.pdf.
[58] Kaitlin Jackson, *supra* note 29.
[59] 389 U.S. 347. (holding that the FBI's wiretapping of a public phone booth violated the suspect's reasonable expectation of privacy).

private-public space distinction and adopted a reasonableness standard.[60] If the suspect exhibits a reasonable expectation of privacy and the public at-large is prepared to recognize that expectation as reasonable, then the government must execute a search warrant before surveilling the suspect.[61]

But discerning what actions are reasonable to a law enforcement officer in the cyber context proves difficult. Courts approach this inquiry by balancing the government's interests in the search and the privacy interests of the individual. If the government's interests outweigh the individual's interests, the search is reasonable. Whether a search is reasonable, however, rests on the assumption that the search is a readily identifiable act over a readily identifiable period of time. This assumption allows courts to categorically determine situations and contexts where society would expect a reasonable expectation of privacy. For example, cars have been held to be less private than homes. Probable cause need only be shown to search a car, but a warrant is almost always needed to search a house.

There are ample exceptions to the need for a search warrant. Relevant to FR gathering, there is the third-party doctrine. When a person hands over personal information to a private third party, that person has presumptively forfeited his reasonable expectation of privacy.[62] United States v. Carpenter, however, has carved an exception to this exception for cell phone data.[63] Another relevant exception is the plain-view doctrine. When a person is engaged in unlawful activity in a manner open for public view, he forfeits his reasonable expectation of privacy.[64] Law enforcement frequently relies on these exceptions to justify big data surveillance of suspects. There are many other exceptions to warrants that are not as relevant to FR data gathering and application.

---

[60] Katz, 398 U.S. at 361 (Harlan, J., concurring).
[61] Id.
[62] See Smith v. Maryland, 442 U.S. 735 (1979).
[63] Carpenter v. United States, 138 S. Ct. 2206 (2018). (holding that given the unique nature of cell phone location records, the fact that the user's data is held be a third party does not overcome the user's claim to Fourth Amendment protection).
[64] United States v. Lee, 274 U.S. 559 (1927).

There are unique contexts whereby courts disregard the existence of a plausible exception. Cell-site data is an example where the data is so intrusive as to outweigh the application of the third-party doctrine.[65] Moreover, government use of technology not available for public use generally has been deemed a search. In Kyllo v. United States, the Supreme Court determined that law enforcement's use of thermal imaging technology to obtain information from the inside of a home constituted a search.[66] Even though law enforcement was on a public street at the time, the use of the thermal imaging to obtain information that would otherwise have required law enforcement to enter the home concerned the Court.[67] Some scholars have considered the application of Kyllo in terms of the limited availability of thermal imaging to FR.[68]

The gathering of biometric nodes alone might pose a Fourth Amendment problem per se. A fair argument could be made that individuals always have a subjective reasonable expectation of their biometric nodes. Individuals have consistently been held to have forfeited their subjective expectation of privacy when walking out in public. But how far does that expectation go? A married couple may not possess a subjective expectation of privacy when promenading through the park, but does it necessarily follow that they subjected themselves to having the measurement between their nose and eyes measured and their skin pores counted? The courts have not ruled on this question yet. However, as the public's awareness of biometric data gathering increases, the societal expectation of privacy decreases; thus, eroding privacy rights.[69]

As big data cybersurveillance grew increasingly sophisticated, judges' frustration with the traditional Katz test kept pace. Courts became jaded by the traditional common law approach,

---

[65] Carpenter, 138 S. Ct. 2206 (2018).
[66] 533 U.S. 27, 33 (2001).
[67] Id. at 34.
[68] See Joseph N. Pato & Lynette I. Millet, *Biometric Recognition: Challenges and Opportunities* 106–107 (2010).
[69] Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, MICH. TELECOMM. & TECH. L. REV. 115, 132 (2005).

yearning for a new, capable set of tools to navigate the legal universe of big data cybersurveillance. These frustrations are best illuminated in Judge Leon's opinion in Klayman v. Obama: "the Smith pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones."[70] As mentioned previously, the principal area of frustration in applying the traditional Fourth Amendment analysis to big data cybersurveillance seems to be the fundamental axiom on which the analysis rests—That all government action can be analyzed as an isolated event. In United States v. Maynard, the D.C. Circuit introduced a different approach dubbed the "mosaic theory" of the Fourth Amendment by legal scholars.[71] Under the mosaic theory, searches can be analyzed as a collective sequence of steps rather than as individual steps. To fully understand the mosaic theory, it is important to flesh out the facts of Maynard and dissect the legal reasoning at the Circuit Court and Supreme Court levels.

IV. The Genesis of the Mosaic Theory

Antoine Jones owned and operated a nightclub in Washington D.C.[72] In 2004 he came under suspicion of drug trafficking and was the main target of a law enforcement investigation.[73] Various methods were used to investigate Jones including visual surveillance of the nightclub and wiretaps on his cell phone.[74] Using the information gathered from these methods, the Government obtained a warrant from the U.S. District Court for the District of Columbia to install a GPS tracking device

[70] 957 F. Supp. 2d at 30-37 (D.D.C. 2013).
[71] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).
[72] United States v. Maynard, 615 F.3d at 549.
[73] Id.
[74] United States v. Jones, 451 F Supp. 2d 71, 74 (D.D.C. 2006), aff'd in part, rev'd in part sub nom. United States v. Maynard, 615 E3d 544 (D.C. Cir. 2010), aff'd sub nom. United States v. Jones, 132 S. Ct. 945 (2012).

(GPS) on the car of Jones's wife.[75] The warrant authorized installation of the device for ten (10) days, but the agents were unable to install the device until the eleventh day.[76] The GPS was installed on the car for twenty-eight (28) days, tracking the vehicle's movements.[77] The GPS communicated Jones's location to a government computer, consisting of 2,000 pages of data over the twenty-eight (28) day span.[78]

Jones was convicted at trial and appealed. The trial court's admission of the GPS evidence was based on the Supreme Court's holding in United States v. Knotts.[79] Knotts permitted the use of a radio beeper located in a car that broadcasted the car's location to the police nearby.[80] The legal theory in Knotts was that an individual who willingly drives on public roads "willingly conveys" to the public that anyone can look at where they're travelling at any time. In other words, Jones relinquished his expectation of privacy when he drove through public roads, therefore, the installation of the GPS did not require a warrant.

Jones argued on appeal that GPS is distinguishable from a beeper.[81] GPS gathers so much data about a person's physical movements across time and space as to intrude into the private details of that person's life. The D.C. Circuit agreed with Jones and reversed his conviction. Judge Douglas Ginsburg first tackled the distinction between GPS and beepers. He explained that Knotts was distinguishable because Knotts did not involve a "dragnet-type law enforcement practice" as used against Jones.[82] Jones's case involved 24-hour surveillance; Knotts's case did not. Ginsburg

---

[75] Jones, 132 S. Ct. at 948.
[76] Id.
[77] Id.
[78] Id.
[79] United States v. Maynard, 615 F3d 544, 568 (D.C. Cir. 2010), aff'd sub nom. United States v. Jones, 132 S. Ct. 945 (2012).
[80] 460 U.S. 276 (1983).
[81] See Brief for Appellants at 54, United States v. Maynard, 615 F3d 544 (D.C. Cir. 2010).
[82] Maynard, 615 F.3d at 556-58 (citing United States v. Knotts, 460 U.S. 276, 283-84 (1983)).

held that that different constitutional principles apply to dragnet-type law enforcement practices like 24-hour GPS surveillance.[83]

Ginsberg's brilliant sleight of hand from Knotts facilitated a smooth transition into the genesis of the mosaic theory—the tool that judges, including Judge Leon, across the country have been longing for. The court held that Jones's movements were not constructively exposed through the observable nature of each individual movement because the whole reveals more than does the sum of its parts.[84] This is where the mosaic analogy comes in. Judge Ginsburg reasoned that individual pieces of data—when viewed collectively—can equal more than the sum of its parts.[85] A single piece of tile in a mosaic is just a single tile, which tells nothing. But if enough tiles are collected, after careful thought, one can paint the whole picture. Because society would find Jones's expectation of privacy over the intimate details of his life over a month-long period to be reasonable, the government's warrantless GPS installation was unconstitutional. The mosaic framework opens the possibility that a series of nonsearches by law enforcement could amount to a search.

The Supreme Court unanimously agreed with Ginsburg's conclusion that Jones was the subject of a search but the rationales differed.[86] Justice Scalia, writing for the majority, held that the installation of the GPS was a trespass on the "effects" of the car, relying on the public-private trespass distinction used frequently prior to Katz.[87] The mosaic theory was never mentioned in his opinion. Five Justices wrote or joined opinions that did, however, touch on the mosaic theory. Justice Alito was joined by four other Justices in his concurring opinion.[88] He found Knotts to be

[83] Id.
[84] Id. at 562
[85] Id.
[86] See United States v. Jones, 132 S. Ct. 945 (2012).
[87] Id. at 951-54
[88] Id. at 957-64 (Alito, J., concurring in the judgment).

applicable but narrowly read Knotts as applying to short-term monitoring of a person's movements. Justice Alito believed that law enforcement was not capable of the twenty-eight (28) day monitoring of Jones without the use of GPS.[89]

Alito's opinion is interesting for a few reasons. Justice Alito applied the reasonable expectation of privacy test by invoking expectations of how law enforcement investigate particular crimes.[90] He argues that society would not consider law enforcement capable of tracking the movements of a vehicle without GPS.[91] Justice Alito does not appear to completely write off the use of GPS tracking in a criminal investigation, however. It is critical to keep in mind that Justice Alito did not consider Jones's offenses "extraordinary." As such, the GPS monitoring was beyond what society would deem reasonable.[92] What makes this reasoning somewhat cryptic is his scant citations to authority. This reasoning seems to shift from what the public might see (i.e., the behavior the individual in question is believed to have engaged in) to what society would expect law enforcement to do given the circumstances. This is a fascinating, nuanced approach considering the mosaic theory has the effect of cracking down on intrusive technologies. But this reasoning suggests that *maybe* BOSS employed by a government agency, paired with the use of other investigatory techniques, could be perfectly legal when used in the context of asymmetric threats. Therefore, with the exception of more serious offenses, society Justice Alito did not find the extensiveness of the search in question reasonable considering the lack of seriousness of Jones's offense.[93]

[89] Id.
[90] Id.
[91] Id.
[92] Id.
[93] Id.

The fifth Justice to apply the mosaic theory was Justice Sotomayor. She reasoned that the use of GPS was unique in that GPS has the capability of shining a light onto the precise details of one's life:[94]

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. 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.[95]

She suggested that individuals have a reasonable expectation of privacy in "the sum of" their public movements.[96] Justice Alito and Justice Sotomayor appear to interpret the mosaic theory slightly differently. Justice Alito focuses on the relation of law enforcement's techniques to the particular crime in question. The more serious the offense, the more extensive techniques the government can employ in its investigation.[97]

Sotomayor's reasoning mirrors Judge Douglas Ginsburg's reasoning. As such, using the previous analogy, BOSS employed by a government agency, paired with the use of other investigatory techniques, may be illegal—even when used in the context of asymmetric threats. This is because Justice Sotomayor appears to focus on the quantity of data collected versus society's expectation of the methods employed by law enforcement when balanced against the offense committed. This is still, however, somewhat cryptic. How much information is too much? How intimate is too intimate? By what standard of intelligence are we measuring the degree of intimacy against? Undoubtedly, a smarter individual is more capable of drawing inferences than less-smart individuals. Questions like these raise the issue of applying Sotomayor and Ginsburg's

[94] Id. at 955-56 (Sotomayor, J., concurring).
[95] Id. at 956.
[96] Id.
[97] See id. at 964 (Alito, J., concurring in the judgment).

version of the mosaic theory. Both Justices, however, measure the collective sum of the government action in determining whether a search occurs—the key takeaway for FRSP's.

Law enforcement has been paying close attention to how the mosaic theory is interpreted by courts. The FBI turned off 3,000 tracking devices shortly after the Jones opinion was handed down.[98] This reflects the effect that the impetus of Fourth Amendment doctrine might be having on the biometric industry in spite of its positive trends. The uncertainty of the mosaic theory, in particular, raises problems. As mentioned, Justice Alito's approach seems to be less restrictive on biometric technology applications in contexts involving serious offenses. In contrast, Justice Sotomayor's approach provides no such safety net. This approach would be problematic for biometric technology providers—and especially FRSP's due to the private nature of faceprints.

V. The Effects of Fourth Amendment Doctrine on Facial Recognition Service Providers

Although the Fourth Amendment has been traditionally applied to state action, FRSP's would be wise to harmonize their gathering methods with Fourth Amendment jurisprudence. The main reason being that most FRSP's, depending on how significantly sales of biometric data contribute to their revenue stream, don't want to risk having to erase their already-stored data and reshape their gathering methods should the courts come along and clamp down on indirect Fourth Amendment abuses. It's not clear that the government is permitted to do something indirectly that is prohibited from doing directly. For example, let's assume the a database a FRSP conveys to law enforcement contains images of persons possessing a reasonable expectation of privacy (i.e., if law enforcement were to have gathered the image, it would have been a violation of the individual's Fourth Amendment right). Can law enforcement access that image without a search warrant? As we already know, there are no statutory restrictions on data brokers selling a person's

[98] Ariane de Vogue, *Supreme Court Ruling Prompts FBI to Turn Off 3,000 Tracking Devices*, YAHOO! NEWS (Mar. 7, 2012), http://news.yahoo.com/supreme-courtruling-prompts-fbi-turn-off-3-154046722--abc-news.html.

personal information directly to law enforcement. But the lack of attention on voluntary data-sharing between law enforcement and the private sector is both problematic and puzzling.[99]

Chief Justice Roberts made clear that if police want access to seven (7) days' worth or more of cell-site data from companies like Verizon or AT&T, a warrant is needed.[100] This logic would seem to apply whether the government is subpoenaing the data or buying it. To be clear, government contracts to purchase data from FRSP's that operate as data brokers do not currently evoke the Fourth Amendment.[101] But in light of Carpenter, there's no telling whether the courts could step in and prevent indirect Fourth Amendment infringements in the future.

FRSP's, especially those operating as data brokers, would be wise to scrape images of persons who have clearly forfeited their reasonable expectation of privacy. For example, photos posted on social media and video surveillance of individuals at parks or malls. Also, FRSP's should limit the amount of information they gather when scraping so as to avoid painting a mosaic of a person's life. For example, the technology should go no further than scraping the biometric nodes and name of the individual. Information such as the individual's employment, education, relationships, or the like should strongly be discouraged from gathering. The technology should be geared to gather biometric nodes and biometric nodes, alone. Keep in mind that individuals currently have no federal cause of action to remove information from a privacy merchant's records.

This advice may not appear to be commercially mellifluous to the ear of a FRSP. On first intuition, the recommendations thus far would appear to render the product less marketable compared to the product containing private, intimate details held by other FRSP's. But consider

---

[99] There are a few exceptions. See e.g., Kiel Brennan-Marquez, *Outsourced Law Enforcement*, 18 U. PA. J. CONST. L. 797 (2016); Eugene L. Shapiro, *Governmental Acquiescence in Private Party Searches: the State Action Inquiry and Lessons from the Federal Circuits*, 104 KY. L. J. 287 (2016); Elizabeth E. Joh, The Paradox of Private Policing, 95 J. CRIM. L. & CRIMINOLOGY 49 (2004); David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165 (1999).

[100] Carpenter, 138 S. Ct. 2206 (2018).

[101] Amitai Etzioni, *Reining in Private Agents*, MINN. L. REV. 279, 282 (2016).

the impetus of Fourth Amendment doctrine in recent years. The idea of purchasing a pandora's box of potentially overly private information may be exactly what the government wishes to avoid. The government doesn't want data that they could not access without a search warrant. More importantly, the government does not want to use data as evidence that eventually falls victim to an exclusionary-rule theory at trial. The government wants to spend precious budgetary resources on reliable, durable data. Also remember that government officials like police officers are employing a vast array of tools in a criminal investigation. Intimate, personal information relating to, for example, a person's job history, banking records, etc., may not just be irrelevant, but redundant. Police departments want to use FR in as limited capacity as possible so as to avoid big-brother depictions by the defense during the prosecution.

This project has laid out potential permanent blockades to government use of FR. What then? Should the federal moratorium, or ban, on FR be signed into law, all hope is not lost for FRSP's. You may recall the discussion at the beginning of this note about how the technology is still developing. Experts believe that as the technology develops, ideas and methods for curbing abuse of the technology will keep pace. Moreover, there is no discussion of banning the sale or manufacturing of the technology itself. Private businesses—in conformity with biometric privacy laws, among others—will always have an interest in using the technology.

What if courts grow overly suspicious of FR and hold that individuals always have a subjective or societal expectation of privacy? In this event, data brokers that have successfully managed to commercialize biometric information may have to diversify their client base. This base could include actors that perform operations in a similar capacity to the government, such as private investigators and security firms. Recall the discussion about the present flourishing of the

facial recognition market.[102] One of the factors driving the market's growth is a rise in defense deployment.[103] FRSP's could assess the needs of military forces and defense contractors to tailor the technology to their needs in an area where U.S. privacy laws are laxer in application.[104]

As it stands, investments in facial recognition technology are on the rise.[105] To maintain this trend, FRSP's would be wise to conform to FTC guidelines as both a legal and—more importantly—a public-relations solution. The biggest threat to facial recognition is the public. If abuse or other corrupt practices draw unwanted attention, the industry may wake the sleeping giant. Investors know this. Bad publicity feeds into the uncertainty surrounding the legality of FR, and too much uncertainty persuades investors to look elsewhere. Tech investors are well-known risk-takers, but only to an extent.

This project has focused mostly on the slippery-slope implications of FR under current law and where the law could take a sour turn for FRSP's. This is due to the trajectory of Fourth Amendment doctrine in recent years. But keep in mind, the reverse could also occur. As time passes, courts could hold that due to the ubiquity of technology and social media and the public's enhanced awareness of private data sharing, we willfully forfeit our Fourth Amendment rights in many contexts.[106] In her book, *Taking Liberties: The War on Terror and the Erosion of American Democracy*, Susan N. Herman says, "familiarity breeds acceptance."[107] She writes, "Once we become accustomed to a new baseline, like bag searches or body scanners at the airport, those practices, like the idea of watchlists, are likely to proliferate."[108] She explains that once these

[102] MarketsandMarkets, *supra*, note 19.
[103] MarketsandMarkets, supra, note 19.
[104] See *Developments in the Law — More Data, More Problems*, 131 HARV. L. REV. 1715, 1722 (2018).
[105] MarketsandMarkets, supra, note 19.
[106] Amitai Etzioni, *supra* note 70.
[107] Susan N. Herman, *Taking Liberties: The War on Terror and the Erosion of American Democracy*. New York: Oxford University Press, 85 (2011).
[108] Susan N. Herman, *supra* note 78, at 85.

measures are introduced, they become commonplace; And we breed an acceptance to these safety measures without truly understanding their effectiveness.[109]

Such an outcome would prove a boon to FRSP's acting as data brokers. With the mosaic theory still holding as the minority position of analyzing Fourth Amendment issues in the context of big data cybersurveillance, FR would meet the Katz test. This is, however, unlikely for a few reasons. For one, the majority of society is still largely unaware of the prevalence and scope of private and public data sharing.[110] This unawareness, however, should not be confused with indifference.[111] Second, such a maneuver would practically scrap the Fourth Amendment completely in a time where technology is the primary tool in criminal investigations. Third, courts prefer leaving sensitive issues such as this to the states. This is another reason why the duration and scope of FR gathering and use is largely at the mercy of public sentiment.

Conclusion

The war between privacy concerns surrounding FR and the utility of FR as a robust crime-fighting tool is a fascinating one. The weakness of privacy regimes at the federal and state level in this area have left staunch privacy advocates to mostly rely on criminal defendants fighting FR on Fourth Amendment theories. A federal ban on government use of facial recognition has been drafted, but in light of the maelstrom of landmark global and domestic events in recent months, public support surrounding its passage remains uncertain. FRSP's operating as data brokers are mostly free to engage in scraping and sell personal information directly to the government but should proceed with caution. Information related to the personal, intimate details of one's life should be avoided in the event the mosaic theory becomes widely

[109] Susan N. Herman, *supra* note 78.
[110] Pew Research Center, *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control over their Personal Information*, (Nov. 15, 2019).
[111] Pew Research Center, *supra* note 76.

adopted. FRSP's should have contingency plans in place in the event the logic in Carpenter extends to contracts between data brokers and law enforcement. These contingency plans should include the diversification of client bases and compliance with the FTC's best practices guideline for facial recognition. The FR market is flourishing, but efforts to avoid investor uncertainty need to improve to maintain these trends.