POWER, PERVASIVENESS AND POTENTIAL: THE BRAVE NEW WORLD OF FACIAL RECOGNITION THROUGH A CRIMINAL LAW LENS (AND BEYOND)

Criminal Courts Committee
New York City Bar Association

August 2020

THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK
42 West 44th Street, New York, NY 10036
212.382.6600 | www.nycbar.org

Power, Pervasiveness and Potential: The Brave New World of Facial Recognition Through a Criminal Law Lens (and Beyond)

The following report from the New York City Bar Association's Criminal Courts Committee provides an overview of facial recognition technology through a criminal law lens. Notably, however, the use of facial recognition technology is not limited to law enforcement: as the world becomes increasingly technology-oriented and technologically dependent, biometrics—and facial recognition in particular—has become pervasive in both the public and private sectors. This paper therefore also delves into related areas and considerations raised by the collection, storage, use and misuse of biometric information, and offers broad policy recommendations to improve facial recognition technology and protect against infringements on personal privacy, constitutional rights, and racial justice.

TABLE OF CONTENTS

I. WHAT IS BIOMETRICS AND HOW DOES IT WORK? 1

II. WHO USES FACIAL RECOGNITION AND WHY? 1

III. CONCERNS THROUGH A CRIMINAL LAW LENS 2

A. Fourth Amendment Search and Seizure Issues 2

B. Fifth and Fourteenth Amendment Due Process Issues 2

C. Fifth Amendment Self Incrimination Issues 3

D. Sixth Amendment Right to Counsel Issues 3

E. Accuracy of Facial Recognition Software 3

F. Perpetuation of Racial Bias and Injustice within the Criminal Legal System 4

G. Widespread, Unbridled and Unbeknownst Use 4

H. Assault on Personal Privacy 5

IV. OTHER CONCERNS AND CONSIDERATIONS 5

A. Impingement on General Human Dignity and Privacy 5

B. Data Security 6

C. Increased Risk of Criminal "Self-Help" 6

D. Financial and Employment Concerns 6

E. First Amendment Free Speech Issues 7

F. Lack of Governing Law 7

V. CRIMINAL AND CIVIL CASES DEALING WITH FACIAL RECOGNITION SOFTWARE AND BIOMETRICS 7

A. SCOTUS 7

B. Federal 7
C. States 9
1. *Virginia* 9
2. *Florida* 10
3. *Illinois* 10
4. *New York State* 11
5. *New Jersey* 11
VI. LEGISLATION AND REGULATIONS DEALING WITH FACIAL RECOGNITION SOFTWARE AND BIOMETRICS 12
A. Federal 12
B. States 14
1. *Illinois* 14
2. *Texas* 15
3. *Washington* 15
4. *California* 16
5. *New York* 16
6. *Arkansas* 17
7. *Massachusetts* 17
C. Cities 18
1. *San Francisco, California* 18
2. *Oakland, California* 18
3. *Sommerville, Massachusetts* 18
4. *Berkeley, California* 18
5. *New York, New York* 18
D. Other Countries 19
VII. PRIVATE SECTOR EFFORTS TO REGULATE FACIAL RECOGNITION AND BIOMETRICS 21
VIII. FUTURE ACTION AND CONCLUSION 21
REFERENCES 23

I. WHAT IS BIOMETRICS AND HOW DOES IT WORK?

- Biometrics is the technical term for body measurements/calculations related to human characteristics.[1] Examples of biometrics include fingerprints, palm prints, facial recognition, DNA, retina/iris, and voice.[2]
- Although it is a technology advanced in the Digital Age, there is evidence of handprint biometrics used as early as prehistoric times as well as in 200s BCE China.[3]
- Biometrics function by comparing a piece of information to a data set to verify one's identity.[4] There are both multi and unimodal biometric systems.[5]
- Facial recognition, one form of biometrics, was pioneered in the mid-1960s.[6] It examines the image of a person's face and measures its specific facial features to find a possible match to a face within a database.[7]
- Facial recognition algorithms work in a variety of different ways: some measure the distance between facial features (eyes, jawbone, etc.), while others use 3D sensors to scan the face, and others analyze skin texture.[8] The facial recognition system then compares this information to a database of faces to find a match.[9]

II. WHO USES FACIAL RECOGNITION AND WHY?

- Generally, biometrics are unique to each individual and thus provide a more reliable identity verifier than "token" or "knowledge" based methods such as ID cards or passwords, respectively.[10] While facial recognition can be less accurate than other biometrics, such as iris or fingerprint scans, it is less invasive, which has contributed to the sharp rise in its use.[11]
- This rise is also attributable to increased law enforcement and surveillance activity in the wake of 9/11.[12]
- Use of facial recognition software has expanded vastly since this time. Some entities that use facial recognition software include:
    - Federal, state and local law enforcement (body cameras, lineups, mugshots, surveillance, etc.), including the Federal Bureau of Investigation (FBI) and U.S. Immigration and Customs Enforcement (ICE);
    - Federal government agencies at airports; the Transportation Security Administration (TSA) monitors passengers entering and exiting airports to identify persons under criminal investigation or persons who have overstayed their visas; TSA and U.S. Customs and Border Protection (CBP) are developing a biometric exit program; there are proposals to make airports 100% biometric;
    - Tech companies (i.e. Apple, Samsung, etc.) to unlock mobile devices;
    - Colleges and universities (to take roll in the classroom, combat cheating, and gain entry to sporting events);
    - Social media companies (i.e. Facebook can identify a photo automatically upon upload);

- Video games (Xbox, Nintendo, etc.);
- Healthcare (i.e. iris scans to identify a non-verbal patient);
- Landlords (to monitor tenants in buildings);
- Music and sports venues (in lieu of scanning tickets);
- Schools and summer camps (to provide security);
- Businesses (to monitor/restrict entrance to certain areas and combat wage theft);
- Retail operations (to identify persons suspected of theft);
- Religious institutions (to take congregation roll and target donation requests);
- Airlines (i.e. faces are scanned in lieu of boarding passes); and
- Marketers and advertisers (i.e. may be used to identify and target certain demographics at concerts, etc.).[13]

- Facial recognition (and other biometrics) are also used in some counties for voter registration.[14]

III. CONCERNS THROUGH A CRIMINAL LAW LENS

- While facial recognition is more secure than token and knowledge-based security systems and has also been employed for positive purposes (including helping law enforcement locate child sex trafficking victims), its use presents a unique host of legal and ethical concerns.[15]

- Facial recognition is unique from other forms of biometric surveillance in the following ways: it tracks something that is difficult to hide and easy to observe in the open (i.e. one's face), there already exist vast name and face databases of law-abiding citizens (i.e. driver's license records) from which to draw datasets, and facial recognition surveillance can be set up using pre-existing camera networks.[16] These factors help to augment the concerns listed below.[17]

A. Fourth Amendment Search and Seizure Issues

- While the Supreme Court has ruled that we have no reasonable expectation of privacy with regard to our outward personal characteristics (i.e. our face, voice, etc.) – and thus a lineup is not a "search" with respect to the Fourth Amendment – it has also held that a police "seizure" of a person for the purpose of subjecting that person to an identification procedure does implicate the Fourth Amendment. [18]
- Biometric "virtual lineups" used by law enforcement agencies across the United States—ever-present, latent identifications of persons not in custody for which reasonable suspicion of criminal involvement may not be present— pose possible Fourth Amendment concerns.

B. Fifth and Fourteenth Amendment Due Process Issues

- The Supreme Court has held that reliability, as opposed to unnecessary suggestiveness, is the key to determining if a criminal identification survives a due process challenge.[19] The factors used to gauge reliability include: the eyewitness's

opportunity to view the suspect, the degree of attention the eyewitness is able to direct to the suspect, the accuracy of any description the eyewitness gave, the time between the crime and identification, and others.[20] Use of facial recognition in "virtual lineups" raises due process concerns as it is unclear if the algorithms making these criminal "identifications" are able to meet these factors – especially in the wake of concerns about their ability to function accurately (these concerns are discussed in the following bullet points).

- Additionally, there exists minimal case law that assesses these factors when a lineup was performed by a computer using facial recognition software.

C. Fifth Amendment Self Incrimination Issues

- In United States v. Wade, the Supreme Court established that the Fifth Amendment protects persons against self-incrimination by *testimonial* acts.[21] Testimonial acts are ones that show a person's mental processes – such as a verbal confession stating "I killed the victim," or telling someone a password or combination to a safe. Wade views a person's physical characteristics – such as a fingerprint, eye color, facial measurements, blood type, handwriting or voice – as non-testimonial, as these characteristics are unique to an individual and largely public.[22] Non-testimonial acts, which include facial recognition and other biometric identification, are thus outside the scope of Wade's Fifth Amendment protections.[23]
- Issues arise, however, when more and more companies use this non-testimonial/physical method of biometric identification in place of mental processes or token-based IDs in order to guard electronic devices that contain a wellspring of sensitive and personal information, as well as information that could be germane to an alleged crime. This issue is discussed, below, with respect to the Baust case and others.

D. Sixth Amendment Right to Counsel Issues

- The Supreme Court has held that a person's Sixth Amendment right to counsel attaches if they appear in a lineup after being indicted, as well as if they appear in a pre-indictment showup.[24]
- It is unclear if these "virtual lineups" are more akin to lineups or showups (i.e. scanning faces in a crowd versus focusing on a single person), however, "virtual lineups" trigger potential Sixth Amendment violations as the right to counsel may attach upon the completion of this virtual identification.

E. Accuracy of Facial Recognition Software

- A 2018 study by a British non-profit found that 95% of facial recognition "matches" by law enforcement wrongly identified innocent people as criminals.[25]
- The Perpetual LineUp (TPL), a study by Georgetown Law's Center on Privacy and Technology, found that only two agencies conditioned the purchase of their facial recognition software on the accuracy of the technology.[26]
- In general, the utility of facial recognition software is dependent on law enforcement officers' understanding of how to use it; yet without specialized training, TPL found that persons making decisions on facial matches are wrong

about half the time.[27] TPL also found that only eight of the facial recognition systems it studied had trained personnel reviewing matches (and it is unclear to what extent this training is regulated).

- Although facial recognition software use is widespread amongst government/law enforcement, it is not subject to any real feedback or testing. While the TSA is proposing to invest significant resources in building largescale surveillance infrastructures at airports, there are no existing standards for the public to assess the accuracy of/provide feedback on such a system; which means that surveillance could increase without any proof that this technology keeps us safer.[28]

F. Perpetuation of Racial Bias and Injustice within the Criminal Legal System

- Federal, state and local law enforcement agencies across the United States use facial recognition software, and it is estimated that 117 million American adults are in facial recognition networks used by law enforcement.[29]
- A 2018 MIT Media Lab study found that facial recognition algorithms designed by IBM, Microsoft and Face++ had error rates of up to 35% or higher when identifying darker-skinned women as compared to lighter-skinned men (for which the error rates were under 1%).[30]
- The American Civil Liberties Union (ACLU) demonstrated the problems with Amazon's Rekognition facial recognition system – a *real time* facial recognition system – when it tested the software on the 535 members of Congress.[31] Amazon's system incorrectly matched twenty-eight congresspersons to criminal mugshots; eleven of these twenty-eight false matches misidentified representatives of color (including the late civil rights pioneer John Lewis).[32]
- In Detroit, where African Americans make up a larger portion of residents than in other sizable American cities, studies showed that facial recognition software used by law enforcement was less accurate when attempting to identify persons with darker skin.[33] These inaccuracies resulted, in part, from the software's homogenous dataset consisting mostly of white, male faces.[34]
- On a general level, facial recognition software has a higher chance of disproportionately affecting African Americans when used by law enforcement as African Americans are more likely to be enrolled in these database systems and subject to their processing.[35] This reality demonstrates how the shortcomings of facial recognition at once exacerbate and reflect the pre-existing racial bias currently plaguing our legal system. One aspect of this racial bias includes the rampant over-policing of African American communities and other communities of color which has resulted in individuals from these communities being incarcerated at higher rates than white individuals.[36]
- These concerns have led some software companies to halt the selling of facial recognition software/biometrics to law enforcement.[37]

G. Widespread, Unbridled and Unbeknownst Use

- Concerns about the use of this technology by individuals are exacerbated by the fact that facial recognition software is at once nascent and burgeoning; the New

York Times published an article detailing how its author built a facial recognition software machine for $60 and installed it in Bryant Park (the facial dataset was composed entirely of photos found on public websites, and existing cameras were used).[38] This machine successfully matched some persons with 89% accuracy and highlights how disturbingly accessible facial recognition software is and how easy it is to track people without their knowledge.[39]

- Law enforcement uses facial recognition technology in body cameras, "virtual lineups," mugshots, surveillance, etc. While it is hard to quantify the exact extent to which facial recognition is used across society, Georgetown's TPL study found that "at least one out of four state or local police departments has the option to run face recognition searches through their or another [agency's] technology . . . [and] . . . [a]t least 26 states (and potentially as many as 30) allow law enforcement to run or request searches against their databases of driver's license and ID photos."[40] This same study also found that, ". . . 16 states let the FBI use face recognition technology to compare the faces of suspected criminals to their driver's license and ID photos, creating a virtual line-up of their state residents . . . " and that "Roughly one in two American adults has their photos searched this way."[41]
- Both the FBI and ICE use facial recognition to scan millions of drivers' license photos in state DMV databases without people's knowledge or consent.[42]
- The New York City Police Department (NYPD) also uses "virtual lineups" to identify teenagers and children using juvenile mugshots as a dataset.[43] These efforts produced proof that the facial recognition system used has a higher risk of false matches for younger faces.[44]

H. Assault on Personal Privacy

- NYPD has access to approximately 9,000 cameras in Lower Manhattan, and the extent of other camera systems used by the Metropolitan Transit Authority (MTA) and New York City Department of Transportation (DOT) is unclear.[45]
- One example cited in Georgetown's TPL concerns Maricopa County, Arizona. Upon purchasing facial recognition software in 2006, the Maricopa County Sherriff's Office merged its driver's license and mug shot databases and the U.S. Department of Justice's (DOJ) booking database with Honduran drivers' licenses and booking photos (provided by the Honduran government) to create a large facial recognition database.[46] Maricopa County did not require reasonable suspicion to run a facial recognition search; furthermore, African Americans are likely overrepresented in the system as they were arrested in Arizona at a rate 170% higher than their population share.[47] Within the Sherriff's Office, a Facial Recognition Unit supervises these searches, and employees are instructed to receive supervisor approval before returning possible results.[48] The TPL, however, found that Maricopa County was not conducting any audits of the system.[49]

IV. OTHER CONCERNS AND CONSIDERATIONS

A. Impingement on General Human Dignity and Privacy

- Some academics – including Italian philosopher and author Giorgio Agamben – argue that biometrics fundamentally and permanently alter the relationship between

individuals and the state, whereby we are subject to perpetual surveillance by the state through ". . . the enrollment and the filing away of the most private and incommunicable aspect of subjectivity: I mean the body's biological life."[50]

- Additionally, this form of tracking/control, historically reserved for persons deemed dangerous or criminal, has ballooned to a widespread, habitual method of state-sponsored surveillance of society at large.[51]
- These concerns are augmented by the normalization of this technology: facial recognition suddenly becomes less threatening when you voluntarily use Snapchat, Facebook, video games, Face ID, etc.[52] This mindset obscures the reality that facial recognition is becoming at once more customary and more latent.
- While some social media companies provide users with instructions on how to opt out of biometrics use with respect to its products, others do not, and it is not always easy to opt out of facial recognition surveillance.[53] This is true on both the macro and micro levels (i.e. at the airport, as TSA expands its biometric efforts and with the rise of the Internet of Things and the rapid escalation of a nearly complete "connectivization" of our lives/households with smart devices through Machine Learning).[54]
- Companies have developed methods such as glasses to disrupt facial recognition software's ability to measure one's face (flu/pollution masks and certain makeup are also effective at disrupting the facial measurement algorithms).[55]
- Large tech companies – such as Google, Facebook and Microsoft – as well as some large R1 Universities have amassed huge biometric data sets (some with millions of images) to develop facial recognition systems.[56] While these entities currently have no legal obligation to disclose these datasets, some have voluntarily shared this information for purposes of further development/research.[57]

B. Data Security

- A security breach could have devastating effects on the personal/financial/medical privacy of millions of people, as well as raise concerns about national security.[58]

C. Increased Risk of Criminal "Self-Help"

- The fact that facial recognition/biometrics are more secure than knowledge or token-based systems may motivate more violent efforts when one wants to gain access to a device secured by biometrics (i.e. physically forcing a person to hold up their face to a scan or cutting off their finger for a fingerprint to gain access, as opposed to stealing a person's key or password).[59]

D. Financial and Employment Concerns

- Some large companies use software that measures job applicants' facial movements, word choices and speaking voice to generate an "employability score" and ranks candidates based on these scores.[60]
- It is unclear what research informs these algorithms and if they are actually accurate/fair/or truly identify which employee will be "best" for a job based on these biometric measurements.[61]

E. First Amendment Free Speech Issues

- In the wake of Freddie Gray's death, the Baltimore Police Department employed facial recognition on social media to identify protestors with outstanding warrants.[62] This use of facial recognition software raises concerns that it could chill free speech.
- Georgetown's TPL observed that of the 52 agencies that it found to use (or have used) facial recognition, only one – the Ohio Bureau of Criminal Investigation – has a policy that expressly prohibits its officers from using facial recognition to track individuals engaging in political, religious, or other protected speech.[63]

F. Lack of Governing Law

- The current legal landscape (discussed below) is all but void of regulations to address the concerns listed above.
- Additionally, the facial recognition market is expected to grow to $7.7 billion in 2022 from $4 billion in 2017.[64] This financial incentive may increase opposition by companies toward government efforts to regulate this technology.

V. CRIMINAL AND CIVIL CASES DEALING WITH FACIAL RECOGNITION SOFTWARE AND BIOMETRICS

- Biometrics and facial recognition are very much unbound technologies that have taken root in an ambiguous legal landscape.

A. SCOTUS

- While there is caselaw addressing technology and Constitutional Rights (i.e. Kyllo v. United States (the use of a heat sensor to see inside a house is a search per the Fourth Amendment); United States v. Jones (placement of a GPS tracker on a car is a search per the Fourth Amendment); Riley v. California (warrantless search of a cellphone is not permissible); and, most recently, Carpenter v. United States (a warrant is needed for seven or more days of historic cell site information/cellphone location data, as such information is analogous to an ankle bracelet for near-perfect surveillance), there is currently no case law that specifically addresses facial recognition software.[65]

B. Federal

- Facebook's DeepFace program – a deep learning recognition system – draws from a database of millions of images uploaded to Facebook and is said to be more accurate than other large-scale facial ID systems.[66] Facebook rolled out DeepFace in 2015 and the system has since been the subject of several class action lawsuits alleging that it violates Illinois' Biometric Information Privacy Act (BIPA),[67] the most recent of which was dismissed for lack of jurisdiction/improper venue.[68]
- In Patel v. Facebook, however, the Northern District of California held that a loss of one's statutory biometric privacy rights is enough to sue a company under BIPA – and that a showing of actual harm is not necessary.[69] Privacy advocates lauded Patel as a huge BIPA victory and its rationale akin to Rosenbach v. Six Flags, a

recent Illinois Supreme Court case, discussed below.[70] Plaintiffs in Patel are claiming $35 billion in damages.[71]

- Facebook appealed Patel to the Ninth Circuit Court of Appeals, claiming that plaintiffs did not have standing to sue, as Facebook's biometric analysis of their photos did not cause them to suffer any concrete harm, and that the district court erred in certifying the class.[72]
- In August of 2019, the Ninth Circuit affirmed the District Court's ruling in Patel, holding that Facebook's violation of BIPA was equal to a violation of the plaintiff's substantive privacy rights and was a concrete injury.[73] In its rationale, the Court looked at the "forest" of recent U.S. Supreme Court Fourth Amendment jurisprudence, which has acknowledged how technology has immensely increased the potential for unreasonable invasion into personal privacy and how these new technologies are not comparable to pre-information age methods of surveillance, etc.[74] It is likely Facebook will appeal this ruling to the Supreme Court.
- There are also a host of class action suits currently pending in the Northern District of California against Facebook in response to the Cambridge Analytica data-sharing scandal.[75] This scandal concerned the secret harvesting of personal data from millions of Facebook pages by British political consulting firm Cambridge Analytica, which it then sold for political advertising purposes.[76]
- Some federal district courts have followed the rationale similar to that outlined in Commonwealth v. Baust – a Virginia state court decision, discussed below – that seems to limit Fifth Amendment protections against biometric use, while others have ruled in the opposite direction.[77] In 2016, a federal magistrate judge in California approved a warrant that compelled a defendant to produce her fingerprint to unlock her phone for the FBI, holding that the unlocking of her phone with her finger was a form of authentication of its contents.[78]
- More recently, however, in early 2019, a Northern District of California magistrate judge denied a portion of a warrant that sought to force persons suspected of an extortion scam on Facebook to unlock their iPhones using their fingerprints.[79] The judge held that technology is outpacing the law at a rapid pace and it is nonsensical that the law considers a verbal communication of a passcode testimonial, and thus worthy of Fifth Amendment protections, and not one's fingerprint or face when used for the exact same purpose.[80]
- This ruling is not binding on any other judge or court in the Northern District of California but is a possible indication of change in how courts view biometrics and Constitutional protections.
- That same year, a federal magistrate judge in the Northern District of Illinois granted the government's application for a search warrant for a residence for child pornography, but rejected its request to compel any persons in the residence at the time to unlock their iPhones with their fingerprints.[81] The court held that compelling production of fingerprints from a large group of people present at the execution of a search warrant to unlock seized devices raised Fifth Amendment concerns, specifically for the failure to establish a connection between any specific

resident and the alleged crime.[82] The court further stated that that an act could qualify as testimonial in nature where ". . . the existence, possession and control, and authenticity of information which tends to incriminate . . ." the person in question.[83] Later in the decision, however, the court emphasized that its ruling was highly fact sensitive and was not meant to mean that the government's request for forced fingerprinting will always trigger equivalent Constitutional concerns.[84]

- While this case has a host of positive treatment, there are many cases that have refused to follow the Northern District of Illinois' In re Application for a Search Warrant. Most recently, in the 2019 In the Matter of A White Google Pixel 3 XL Cellphone in a Black Incipio case, the United States District Court of Idaho refused to follow In re application for a Search Warrant, stating that a warrant compelling someone suspected of possession of child pornography to unlock his phone with his finger *did not* violate his Fifth Amendment rights.[85] While it acknowledged the intensity of privacy rights associated with today's cell phones and biometric data, the court in White Google Pixel looked to a host of recent similar cases across district courts which based their rulings in Wade's (and its robust progeny's) notion that the Fifth Amendment Right Against Self-Incrimination protects people against the government compelling them to make *testimonial* acts – or acts that display "the contents of one's own mind."[86] The court concluded that pressing one's finger to a phone, "is simply the seizure of a physical characteristic". . . [and] . . . there is no need to engage in the thought process of the subject at all in effecting the seizure . . .. [as] . . .the fingerprint by itself does not communicate anything."[87]
- On the macro level, White Google Pixel, displays the divergence of federal jurisprudence on Fifth Amendment issues and biometrics and highlights how a well-informed Supreme Court decision might provide much-needed direction on this issue.

C. States

1. *Virginia*

- In Commonwealth v. Baust, a Virginia state trial court held that while police cannot compel a suspect to provide his passcode to unlock his smartphone – as this is a violation of the Fifth Amendment right against self-incrimination – the police *can* compel that same suspect to produce his fingerprint to do the same.[88] Baust distinguishes physical-based (i.e. fingerprint) security from testimonial security (i.e. providing someone with a verbal or written password), deeming it outside the scope of Fifth Amendment protections against self-incrimination.[89]
- Specifically, the judge in Baust held that producing one's fingerprint did not require the communication of knowledge, but rather is more akin to being ordered to produce something physical – such as a DNA sample or a key to a safe – which is permitted per United States v. Wade (which holds that the Fifth Amendment "offers no protection against compulsion to submit to fingerprinting)."[90] Wade deems an act to be "testimonial," and thus worthy of Fifth

Amendment protections, when law enforcement forces a person to reveal his knowledge of facts, thoughts and beliefs relating him to the offense (i.e. "the content of his own mind"); a fingerprint is not testimonial as it does not require the defendant to "communicate any knowledge at all."[91]

- While several recent cases refused to follow Baust, a host of recent state rulings reference Baust and mirror its rationale of the Fifth Amendment's testimonial privilege and biometrics. In 2017, the Minnesota Supreme Court held in State v. Diamond that the Fifth Amendment does not protect a person from being ordered to provide a fingerprint to unlock a seized cellphone because the compelled act is not a testimonial communication.[92] Like Baust, the court's decision hinged on the proposition that providing a fingerprint elicits only physical evidence from a suspect's body and does not reveal the contents of the person's mind.[93]

2. ***Florida***

- In 2016, a Florida district court cited Baust in Florida v. Stahl, where it held that compelling a fingerprint to open an iPhone is not protected by the Fifth Amendment.[94]
- Recently, a Florida state appellate court held that a defendant/appellant had no right to view photos of other suspects identified by FACES, a facial recognition software whose search produced a "one star" ID match of the defendant that led to his arrest.[95] FACES' ID match was not subject to any accuracy audits.[96] This case raises several constitutional issues (i.e. Brady Disclosure, Sixth Amendment issues, Daubert issues, etc.) and was appealed to Florida's Supreme Court.[97]

3. ***Illinois***

- BIPA has been the subject of a host of lawsuits by tech giants – such as Google and Facebook – although these efforts, as of this date, have not yielded any success for them. Facebook has also spent considerable resources lobbying to amend/restructure BIPA.[98]
- In response to BIPA's most recent challenge in Rosenbach v. Six Flags – where parents sued Six Flags upon learning that the amusement park fingerprinted their fourteen year old son without their consent – the Illinois Supreme Court found in favor of the family when Six Flags sued to have the suit dismissed.[99] The court disagreed with Six Flags' argument that BIPA required that one show an injury beyond loss of statutory privacy rights, and held that that a finding of actual harm under the BIPA was not necessary for purposes of being "aggrieved" and the plaintiffs could proceed with their class action against the park.[100] The court held that merely

losing one's biometric privacy is sufficient enough harm for purposes of proceeding with an action under BIPA.[101]

- While advocates lauded Rosenbach as a crucial victory in the fight to preserve personal privacy, critics voiced concerns that it will only encourage what some consider the recent onslaught of BIPA litigation in Illinois in the wake of this lessened standard of harm necessary to pursue a case; over 200 BIPA cases were filed in the two years before Rosenbach, and some of the larger tech companies, such as Facebook, are facing possible damages in the billions.[102]
- In response to BIPA/Rosenbach, some companies have started including provisions requiring consent to biometric security in employee handbooks.[103]

4. ***New York State***

- In 2009, the Court of Appeals ruled in People v. Weaver that the police must first obtain a warrant before tracking a person's vehicle with a GPS device as it violates the Fourth Amendment protection against unreasonable search and seizures (basically establishing Jones protections three years before SCOTUS).[104]

5. ***New Jersey***

- In State v. Andrews, the New Jersey Superior Court held that testimonial aspects of passcodes required to unlock a defendant's smartphones were a "foregone conclusion," and thus compelled production of passcodes did not violate the defendant's Fifth Amendment privilege against self-incrimination under this exception.[105]
- In this regard, Andrews treats Baust negatively in that Baust held that a "password is not a foregone conclusion because it is not known outside of [the defendant's] mind."[106]

- Like the federal landscape, the state jurisprudence is also very divided on the issue of Fifth Amendment protections and biometrics and federal guidance could help bring consistency.
- There seems to be a lag in jurisprudence with respect to assessing the functionality, as opposed to the physicality, of biometrics as it relates to guarding against self-incrimination. One might argue that while, singularly, a finger print is a physical part of your body, Baust/White Google Pixel/etc. ignore the marked rise in the use of biometrics for forensic passwords/identification as they are harder to fake and better at guarding sensitive information. Viewed in this way, a fingerprint may be more analogous to a password than a key.
- While it is true that, like a key, a fingerprint is a physical thing (versus a testimonial verbalization of a thought), it is the *use* of this fingerprint and its potential to extract incriminating evidence from a smartphone, for instance, on which the Fifth Amendment analysis should turn. The intended use (function) should be more significant than the physicality (form). Thus, if fingerprints are being used to unlock a device in order to

explore the device's contents, law enforcement should not be permitted to compel persons to do so because this act is tantamount to providing a password and therefore, in effect, testimonial.

- To these points, when the Supreme Court decided Wade in 1967, computer technology was in its infancy. An updated Supreme Court decision that distinguishes/extends Wade's definition of a "testimonial" act to include biometrics identifiers would be appropriate to protect our Constitutional rights in the Digital Age.

VI. LEGISLATION AND REGULATIONS DEALING WITH FACIAL RECOGNITION SOFTWARE AND BIOMETRICS

- Regulation of facial recognition technology/biometrics can apply to the use, storage or retention of biometric data, as well as to the formal technology itself; however, the current regulatory landscape is inadequate across federal, state and local jurisdictions. This reality augments the concerns listed above.

A. Federal

- Currently, there exists no federal, all-encompassing law that protects user privacy and regulates the storage of personal data (biometric or other) by the private sector.[107]
- The Electronic Communications Privacy Act of 1986 (ECPA) is a federal statute that sets standards for government monitoring of cell phone and internet communications.[108] This law, however, deals more with storage of personal data, rather than limitations on the biometric technology itself.[109] It was also passed long before the extreme technological advancements of the past twenty-five years and thus has many shortcomings with respect to protecting people's privacy.[110]
- 18 USC 2703(d) allows the government to obtain third party electronic data (i.e. data from Facebook, Uber, Verizon, etc.) if it "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[111] This 2703(d) standard is a much lower bar than obtaining a warrant with probable cause. As with the ECPA, however, this law deals more with long term surveillance/third party/Carpenter surveillance issues (discussed in the pages below), rather than biometrics specifically.
- Senators Roy Blunt (R-MO) and Brian Schatz (D-HI) have introduced the Commercial Facial Recognition Privacy Act of 2019 (S.847), or CFRPA, which would require consent before using biometric ID/tracking on individuals by businesses, but *does not* apply to local, state or federal governments.[112]
- In late 2019, Senator Maria Cantwell (D-WA) introduced the Consumer Online Privacy Rights Act (S.2968), or COPRA, the first ever comprehensive federal consumer privacy law.[113] COPRA establishes data and privacy protections, including the right to access and delete one's personal data held by an entity, and protects individuals by imposing data security requirements on companies to ensure their practices are sufficient to safeguard personal data.[114] Additionally, COPRA

establishes a private right of action for individuals to sue in the event a company violates their privacy as well as empowers state attorneys general to enforce the law.[115]

- In July of 2019, U.S. Representative Yvette D. Clark (D-NY-9) introduced the No Biometric Barriers to Housing Act (H.R. 4008), which would ban the use of biometric technology, including facial recognition, in certain federal rental units.[116] H.R. 4008 is co-sponsored by Representative Rashida Tlaib (D-MI-13), whose constituents in Detroit have voiced concerns about large scale facial recognition technology use in federal public housing by law enforcement.[117]
- In late June of 2019, Representative Michael McCaul (R-TX-10) and Senator Martha McSally (R-AZ) introduced the Biometric Identification Transnational Migration Alert Program Authorization Act of 2019 (H.R. 3377/S.1933). These bills direct federal funds to amend the Homeland Security Act of 2002 to establish the Biometric Identification Transnational Migration Alert Program (BITMAP) in the Department of Homeland Security.[118] BITMAP calls for the use of facial recognition and other biometric data to enhance border security.[119] The bills direct the U.S. Department of Homeland Security to coordinate with the U.S. Secretary of State, foreign governments, and other Federal agencies, as appropriate, to voluntarily share biometric information collected by foreign nationals in order to screen these persons to identify any potential threats to the United States.[120]
- While H.R. 3377/S.1933 touch on how biometric data of U.S. citizens captured by BITMAP should be expunged from all databases, it makes an exception to retain this data ". . . for specific law enforcement or intelligence purposes." [121] This exception seems vague and outlines no other details on how the law would curb potential abuses caused by the unbridled gathering of biometric data by the government/law enforcement.
- It is important to note that, with the exception of the No Biometric Barriers to Housing Act (H.R. 4008), the aforementioned federal legislation does not attempt to regulate facial recognition technology itself, but rather proposes limits on the manner in which biometric data is collected/stored. While there are some other federal bills that mention biometric identification, none propose to regulate this technology directly. Additionally, H.R. 4008 does not provide for any kind of uniform/industry-wide standards for facial recognition itself, but rather proposes restrictions on biometrics in a specific situation.[122]
- While the National Institute of Standards and Technology (NIST), a branch of the U.S. Department of Commerce, administers the Face Recognition Vendor Test (FRVT), which tests the accuracy of facial recognition software in different scenarios and across various demographics (i.e. age, race, gender), this test is voluntary. The overall role of the NIST is to gather data rather than promulgate regulations.[123] NIST allows companies to send one submission for FRVT assessment every four months.[124]

B. States

- Most states have not passed any laws regulating biometrics/facial recognition technology. This type of data is being regulated by existing privacy laws, which are not best postured to address the concerns posed by this technology (discussed above). Facial recognition data may be regulated per a privacy policy so long as there is no direct regulation/restriction by a specific federal law (i.e. HIPPA, Privacy Act of 1974, etc.). There are a handful of states, however, that are making efforts to reign in biometrics.
- An important distinction across these various state laws is that some – like Illinois' Biometric Information Privacy Act (BIPA) – create a private right of action for individuals, or classes, to enforce the law and seek damages, while others, like the California Consumer Privacy Act (CCPA), provide a limited right of action; others are only enforceable by a state's attorney general.[125]
- How states define "biometric information" varies as well. Under the CCPA, it is broadly defined to include physiological, biological, and behavioral characteristics – such as also keystroke and gait patterns as well as certain sleep and exercise data – while BIPA and Texas's Biometrics Privacy Law have a more traditional definition – limited to things such as fingerprints, voiceprints, iris and facial scans.[126]
- There has been a recent trend with respect to states proposing laws that would limit the use of facial recognition and biometric identification technologies, including Alaska, Arizona, Florida, Michigan and Delaware.[127] Even within these efforts, however, there is divergence between these proposed laws, and perhaps some kind of federal legislative floor is necessary to ensure a uniform statutory landscape.

1. *Illinois*

- Illinois passed BIPA in 2008, back when Facebook was still in its relative infancy and most companies were not thinking about face-recognition technology.[128] It was the first state in the country to do so.[129] BIPA requires that entities obtain affirmative consent from individuals before obtaining their biometric information and creates a private right of action for individuals to sue to enforce the law.[130]
- Under BIPA, a prevailing party may recover actual damages or liquidated damages of $1,000, whichever is greater, *for each violation.*[131] If the violation is intentional or reckless, however, these liquidated damages go up to $5,000 per violation.[132] Injunctive relief and reasonable attorney fees and costs, as well as expert witness fees and other expenses, are also available to a prevailing party.[133]
- While BIPA has its critics, aims to hold accountable an industry that for years has been collecting individuals' biometric information with near-total impunity.

2. *Texas*

- Texas's 2009 Biometrics Privacy Law defines "biometrics" as more traditional physical characteristics (i.e. voice, face, fingerprints, etc.). and allows for civil penalties of up to $25,000.[134] Unlike BIPA, however, only the Texas Attorney General can enforce biometric privacy violations.[135]

3. *Washington*

- In 2017, Washington passed House Bill 1493, becoming only the third state in the country to pass legislation regulating the use and collection of biometric information.[136] HB 1493 defines "biometric identifier" as data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual.[137]
- Unlike the Illinois and Texas statutes, HB 1493's definition of "biometric identifier" excludes facial recognition data.[138]
- Currently, the proposed Washington Privacy Act (SB 5376) would allow consumers the right to access and manage their biometric data held by companies.[139] The law also proposes setting standards for the use of facial recognition technology.[140] As of January 2020, this bill is still in committee and several amendments have been proposed.[141]
- By way of House Bill 1071 (HB 1071), Washington recently expanded its existing data breach response law to include biometric data in its definition of personal information.[142] Passed in May of 2019, HB 1071 goes into effect in May of 2020.[143]
- This new definition of "personal information" is expansive and includes: "Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "[144]
- HB 1071 also expands the reporting requirement for entities that "maintain *or possess* [emphasis added]" personal information; they now must notify affected person(s) of any breach in security with regard to the maintenance of such information.[145] The law requires that an entity must also notify the Washington Attorney General in the event of a data breach that impacts more than 500 people within 30 days of discovery of such breach.[146]
- HB 1071 makes an exemption to the notification requirement when a data breach "is not reasonably likely to subject consumers to a risk of harm" or when data was acquired in good faith.[147] The law defines a "good faith acquisition of personal information" as when "the personal information is not used or subject to further unauthorized disclosure."[148]

4. ***California***

- In mid-2018, California passed the CCPA which allows Californians more control over their biometric data.[149] The law allows persons to see which information businesses collect on them, request this data be deleted, see to whom their data is being sold, and lets persons stop this data from being sold if they so choose.[150] Set to go into effect in 2020, CCPA also requires that companies get users' permission before collecting data.[151]
- The CCPA amends California's definition of personal information to include biometric data, which the CCPA broadly defines to include physiological, biological and behavioral characteristics.[152]
- Facebook, Google and other software/social media entities vehemently opposed the CCPA, and its previous iterations.[153] Big Tech lobbyists have chipped away at the language in the bill to lessen companies' responsibilities to protect personal information (i.e. including a stipulation that businesses must include a clear button on their websites giving people the ability to opt out of data collection and the requirement that businesses share "accurate names and contact information" for third parties that bought user data over the prior year.[154] That language has since changed, requiring businesses to merely disclose the "categories of third parties" that bought the data).[155]

5. ***New York***

- New York's proposed Biometric Privacy Act (A.1911/S.1203) provides regulations for entities that store biometric data.[156] Specifically, private entities in possession of biometric data would have to develop written record retention schedules and guidelines for permanently destroying biometric data "when the initial purpose for collecting or obtaining data has been satisfied or within three years of someone's last interaction with the company, whichever is earlier."[157]
- Like BIPA, the Biometric Privacy Act also proposes a private right of action,.[158] This bill has failed to gain traction and opponents argue that it was a way for abuse by class action lawyers.[159]
- While New York recently updated its data breach law to include biometric data in its definition of "personal information" (discussed, below), biometric technology itself is not currently regulated directly; however, the New York Department of Labor prohibits the use of forced fingerprinting, "unless allowed by law."[160] This law often affects employers who want to use biometric timeclocks to combat wage theft.[161]
- In July of 2019, Governor Cuomo signed A.5635-B/S.5575-B – the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) – into law.[162] The SHIELD Act updates New York's data breach

notification law, expanding the types of covered personal information to include biometric data that would trigger notification obligations for entities in possession of "personal information" in the event of a data breach.[163] SHIELD also broadens the data breach notification requirement by mandating notification of unauthorized access *to* protected information, rather than just the acquisition of data.[164] While the law does not create a private right of action, it does authorize the New York State Attorney General to seek civil penalties for non-compliance.[165]

- The proposed A.7790/S.5687 prohibits the use of a facial recognition system by a landlord on any residential premises.[166]
- In Brownsville, Brooklyn, tenants of two rent-stabilized apartment complexes recently filed a complaint with the New York State Department of Homes and Community Renewal to enjoin their landlord from installing facial recognition entry systems in their buildings.[167] While the landlord claims these new systems are to ensure tenant safety, tenants insist that their buildings already have sufficient security and cite personal privacy concerns.[168]
- In the current legislative session, there is a wave of proposed legislation that aims to limit the use of biometrics/biometric data.[169] One of these bills includes A.9767/S.7572.[170] The bill proposes prohibiting the use of biometric surveillance by law enforcement, as well as establishing a biometric surveillance regulation task force.[171]
- While many of these proposed bills regulate data and/or limit the way/scope in which facial recognition/biometrics can be used, A.8042, S.5140 and S.6623 (and a few others) call for a fundamental, information-gathering process for biometrics in order to better understand this technology so that it can be more effectively regulated.[172] There currently exists no analogous legislative efforts at the federal level.

6. *Arkansas*

- In April of 2019, Arkansas passed House Bill 1943 (HB 1943), which amends the state's Personal Information Protection Act to include biometric data in its definition of "personal information."[173] HB 1943 also amends the State Code, requiring an entity in the possession of personal information to notify the Attorney General in the event of a data breach which affects the personal information of more than 1,000 individuals.[174] This bill is similar to the efforts recently taken by Washington's HB 1071, described above.

7. *Massachusetts*

- There are currently two bills pending in the Massachusetts legislature (H. 1583 and S. 1385) that would impose a moratorium on government use of biometric surveillance – including facial

recognition – until laws are passed regulating who may use it and how.[175]

C. Cities

1. *San Francisco, California*

- In mid-May of 2019, San Francisco passed a municipal ordinance banning the use of facial recognition technology, becoming the first city in the United States to do so.[176]
- The grassroots coalition that advocated for the passage of this ordinance cited civil liberties concerns, including widespread use by federal ICE agents, privacy concerns, and perpetuation of racial injustice as reasons for the need to ban facial recognition.[177]

2. *Oakland, California*

- Oakland banned facial recognition technology in July of 2019.[178]

3. *Sommerville, Massachusetts*

- In June of 2019, Sommerville's City Council banned the use of facial recognition technology in police investigations and municipal surveillance programs.[179]

4. *Berkeley, California*

- In mid-October of 2019, Berkeley, California joined its neighbors and passed a ban on all government use of facial recognition technology.[180]

5. *New York, New York*

- The New York City Council recently passed Int. 0487A-2018 (also referred to as the Public Oversight of Surveillance Technology (POST) Act) and it was enacted into law on July 15, 2020.[181] The POST Act increases oversight of the NYPD's use of surveillance technology by requiring reporting and evaluation of surveillance technologies used by the NYPD.[182] It will require the NYPD to draft a surveillance impact and use policy which will be subject to a public comment period.[183]
- In late 2018, New York City Councilman Ritchie Torres, head of the council's Committee on Oversight and Investigations, introduced Int. No. 1170-2018 that would regulate biometric use, to a degree.[184] The bill would amend Section 1, Chapter 5 of Title 20 of the City's Administrative Code and require businesses to provide notice to persons if they are collecting what the bill defines as biometric data.[185] The bill would not, however, apply to government agencies.[186]
- Like BIPA, Int. No. 1170 also creates a private right of action and allows for a prevailing party to recover damages of $1,000 per

violation against a negligent entity and $5,000 per violation against an entity that was reckless/intentional, and allows for attorney's fees and "other relief," including injunctive relief, "that the court deems appropriate."[187]

- Additionally, Int. No. 1170 gives the commissioner of the New York City Department of Consumer Affairs authority to implement a civil penalty of $500 per day for a violation.[188]
- It is important to note that Int. No. 1170 *does not* apply to government entities; this means that the plethora of constitutional concerns, discussed above, are not addressed by this bill.[189] Critics on the other side of the spectrum have voiced concerns that Int. No. 1170 will lead to a BIPA-like influx of litigation.[190]
- In related efforts, Councilman Brad Lander introduced Int. No. 1758-2019 in October of 2019. [191] This law would define the word "key" in the City Code and require that building owners provide mechanical keys to residents for both the exterior door of their buildings and the doors to their individual apartments.[192] It would also prohibit landlords from forcing tenants to use keyless entry technology to enter their buildings.[193]
- In August of 2019, Councilman Donovan J. Richards introduced Int. 1672-2019, which requires real property owners to submit registration statements regarding biometric recognition technology utilized on the premises.[194] The bill would also require the City's Department of Information Technology to establish a database and provide an annual report to the Mayor and the City Council.[195]

D. Other Countries

- The European Union (EU) has been more proactive than the United States with respect to regulating biometric data. In 2016, it passed the General Data Protection Act (GDPA), the world's strongest data protection law, which came into force in mid-2018.[196] One of the goals of the GDPA is to modernize data protection and institute uniformity across the EU's legal landscape.[197]
- The GDPA contains ninety-nine articles that outline the rights of individuals and obligations placed on organizations covered by the law and establishes a penalty scheme and responsibility for organizations to obtain the consent of persons from whom they collect personal data.[198]
- The GDPA defines "personal data" as ". . . any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . . ." [199]
- The United Kingdom passed its own version of the GDPA – the Data Protection Act of 2018 – which largely mirrors the EU's law, in anticipation of Brexit.[200] It

currently has no law, however, regulating the formal use of biometric facial recognition cameras, specifically.[201]

- In contrast, the London police force recently instituted a large-scale camera network used for a "perpetual lineup."[202] These efforts have been met with protest and pending legal challenges.[203]
- In other counties, use of facial recognition is more widespread. In China, you can use facial recognition to order fast food, while police officers have also begun wearing glasses with facial recognition capabilities that allow them to track and identify individuals within large crowds.[204]
- Chinese tech giant Huawei has installed its "Safe Cities" facial recognition monitoring system in cities across the globe where Chinese companies have made recent, large-scale business investments (such as Belgrade, Serbia and Kampala, Uganda, among others).[205] These countries often have less power and military infrastructure than China.[206] In the wake of these efforts, citizens of these nations have voiced privacy concerns, which have been augmented by claims that Huawei's facial recognition systems will give China unfettered access to its data (because of accusations of government control of the company) which could compromise the privacy of people in poorer countries that may not have the power to stand up to China.[207] If the people in these nations speak out against China or act in ways that China deems threatening to its business interests, critics claim that China could easily spy on them using Safe Cities technology and crush dissent.[208] "Safe Cities" is an example of how government and private entities might use facial recognition software to impinge on human rights and repress dissent. Huawei's "Safe Cities" systems are found in some 230 cities worldwide.[209]
- Aadhaar – India's national ID program – is the world's largest biometric database.[210] It holds profiles of people for their lifetime and was designed to help government agencies deliver public services securely, to a large group of people, using biometric and demographic data.[211]
- Over 500 million residents are enrolled in the system; however, Aadhaar has come under fire from critics because of data security concerns, errors in record keeping which have led to injury and death, and a general concern about personal autonomy/privacy. These concerns led India's Supreme Court to establish privacy as a fundamental right.[212]

- Some academics and others have called for a complete ban on facial recognition because of its power, pervasiveness and potential to completely and permanently alter the dynamic between individuals and the state with respect to personal privacy.[213] They argue that industry guidelines and even legislation itself cannot curb potential abuses of this technology (although a ban at this point seems unfeasible, as the use of facial recognition use is so widespread).[214] Other arguments favor more regulation, as a ban would prohibit positive uses of the technology.[215]

VII. PRIVATE SECTOR EFFORTS TO REGULATE FACIAL RECOGNITION AND BIOMETRICS

- At this time, no industry-wide standards exist that would allow for uniform biometric technology use. While some companies have made efforts to combat bias and inaccuracy in facial recognition software (e.g., IBM is introducing a more diverse dataset in the hopes of combating AI bias), it is unclear how impactful these efforts are.[216]
- Additionally, while not all companies are forthcoming about these efforts, others are informing the public of their contributions to researching and combating these issues.[217]
- Alternatively, Amazon, which came under fire in the ACLU's report of racial bias in its Rekognition facial recognition system, stated that it would not stop selling the software to a host of government and law enforcement agencies, even in the wake of complaints voiced by its own employees.[218] Amazon also refused to have NIST assess Rekognition.[219]
- A February 2019 blog post by Michael Punke, VP of Global Public Policy at AWS, highlights Amazon's concerns associated with AI and called for regulations to increase transparency in its use.[220]
- In 2018, after backlash from its participation in Project Maven – a Pentagon drone project – Google announced that it would no longer work on AI weapons projects and released a set of ethical guidelines for AI use and development (although it continues to work with the US military).[221] Google's own employees have also voiced concerns about Google's involvement with this project, with some resigning in protest.[222]
- The Institute of Electrical and Electronics Engineers, a large professional organization, has authored *Ethically Aligned Design*, a treatise on ethics in AI, and have created a global initiative to set standards to combat AI bias.[223]
- Joy Buolamwini – the researcher at MIT's Media Lab who discovered high rates of racial bias in a host of recognition algorithms – created the Algorithmic Justice League (AJL) to raise awareness of racial bias in biometric systems and work to combat this issue.[224]
- In an op-ed in the New York Times, House minority Leader Kevin McCarthy (R-CA-23) urged that trustbusting of large tech companies is not the answer to guarding against data breaches but, rather, urges a public/private sector partnership that incorporates technologies such as Cryptonetworks (decentralized platforms governed by the community of users themselves).[225] In Cryptonetworks, data would be controlled by blockchain encryptions, rather than the platform itself. McCarthy also calls for Congress to set a federal standard for privacy frameworks.[226]

VIII. FUTURE ACTION AND CONCLUSION

- Facial recognition is, at once, an emerging and rapidly advancing technology that is widely-used with a regulatory framework insufficiently postured to deal with the grave risks it poses to personal privacy, constitutional rights, and racial justice. These issues take the form of a frightening legal Venn diagram that merges two of the most pressing issues currently facing the legal profession: in one circle you find mass incarceration/racial injustice, and in the other, the inability of society to pass laws and issue judicial decisions that keep pace with technology.

- Considering the disjointed judicial landscape, this issue – particularly with respect to Fifth Amendment testimonial protections – is ripe for Supreme Court intervention, however it has no relevant cases on its docket.
- More uniform, comprehensive federal laws are also needed to fill the regulatory void and set minimum accuracy standards across the industry to attempt to curb the bias that infects facial recognition and other biometric technology.[227] The legislative scheme of this industry must also be changed from voluntary to mandatory.
- Augmenting NIST into a true regulatory agency will be crucial with respect to reforming our ability to regulate biometrics as this will allow for enhanced oversight of this industry as well as registration, training and testing of this software. While many of these deep learning algorithms that fuel biometric systems are challenging to send for analysis, because they are extremely large and update in real time, some sort of technological/regulatory scheme needs to be established such that NIST can properly test these systems for bias.[228] One solution may be that NIST establish a corps of inspectors who can travel to facilities to test software.
- This complex and wide-reaching technology may be best regulated through a multi-pronged approach that applies to both government and private entities.[229]
- While addressing the concerns presented by facial recognition and biometrics is an immense undertaking, these efforts present an opportunity for the legal profession to protect individuals' personal privacy and advance justice for society at large.

REFERENCES

[1] *What is Biometrics?*, Biometrics Research Group of Michigan State University, http://biometrics.cse.msu.edu/info/index.html (all websites last visited July 21, 2020).

[2] *Id*.

[3] *The History of Fingerprints*, onin.com, http://onin.com/fp/fphistory.html.

[4] *What is Biometrics?*, *supra* note 1.

[5] *See* Tarun Choubisa, SR Mahadeva Prasanna and Soyuj Kumar Sahoo, *Multimodal Biometrics Person Authentication: A Review*, IETE Tech. Rev. 2012, https://www.tandfonline.com/doi/abs/10.4103/0256-4602.93139?journalCode=titr20; *See* Danny Thakkar, *Unimodal Biometrics vs. Multimodal Biometrics*, BAYOMETRIC, https://www.bayometric.com/unimodal-vs-multimodal/ (describing how unimodal biometric systems measure one biometric trait [such as voice] while multimodal biometric systems measure two or more biometric trait [such as fingerprint and voice]).

[6] *See* Laura Blanc, *The Face of the Future*, Herta, Dec. 14, 2014, http://www.hertasecurity.com/en/node/210.

[7] *Id*.

[8] *See* Steve Symanovich, *How Does Facial Recognition Work?*, Norton, https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html; *See* Mark Williams Pontin, *Better Face-Recognition Software*, MIT Technology Review, May 30, 2007, https://www.technologyreview.com/2007/05/30/225291/better-face-recognition-software/; *See* Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work – 3D Facial Recognition*, How Stuff Works, https://electronics.howstuffworks.com/gadg ets/high-tech-gadgets/facial-recognition2.htm.

[9] *Id*.

[10] Danny Thakkar, *Biometric Regulations in the U.S. States: The State of Play*, BAYOMETRIC https://www.bayometric.com/biometric-regulations-us-states/.

[11] Danny Thakkar, *Top Five Biometrics: Face, Fingerprint, Iris, Palm and Voice*, BAYOMETRIC, https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/.

[12] Jay Stanley, *How the TSA's Facial Recognition Plan Will Go Far Beyond the Airport*, ACLU, Oct. 23, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/how-tsas-facial-recognition-plan-will-go-far; *See, The Five Problems with CAPPS II*, ACLU, https://www.aclu.org/other/five-problems-capps-ii; *Testimony of Deputy Assistant Secretary for Policy Kathleen Kraninger and Director Robert A. Mocny Before the House Appropriations Committee and Subcommittee on Homeland Security and "Biometric Identification,"* Mar. 19, 2009, https://www.dhs.gov/news/2009/03/19/testimony-biometric-identification; *See* Transportation Security Administration, *TSA Biometrics Roadmap*, Sept. 2018, https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

[13] Stanley et. al., *supra* note 12.; Symanovich, *supra* note 8.; Julie Jargon, *Facial Recognition Tech Comes to Schools and Summer Camps*, The Wall Street Journal, Jul. 30, 2019, https://www.wsj.com/articles/facial-recognition-goes-to-camp-11564479008; Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, The Washington Post, Jul. 7, 2019, https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/; Catie Keck, *United Airlines is Expanding Its Creepy Biometric Screening Technology to More Airport Hubs*, Gizmodo, Jul. 29, 2019, https://gizmodo.com/united-airlines-is-expanding-its-creepy-biometric-scree-1836789894; *See UT Introduces Advanced Biometric Security for Quick Access to Games*, KXAN, Oct. 18, 2019, https://www.kxan.com/news/local/austin/ut-introduces-advanced-biometric-security-for-quick-access-to-games/.

[14] International Institute for Democracy and Electoral Assistance, *Use of Biometric Data in Voter Registration*, https://www.idea.int/data-tools/question-view/738.

[15] *See* Tom Simonite, *How Facial Recognition Is Fighting Child Sex Trafficking*, Wired, Jun. 19, 2019, https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/amp.

[16] Sahil Chinoy, We Built an 'Unbelievable' (but Legal) Facial Recognition Machine, The New York Times, Apr. 16 2019, https://www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html.

[17] *Id*.

[18] *See* United States v. Dionisio, 410 U.S. 1, 14 (1973); Hayes v. Florida, 470 U.S. 811, 816 (1985); Davis v. Mississippi, 394 U.S. 721, 724 (1969).

[19] *See* Neil v. Biggers, 409 U.S. 188 (1972).

[20] *Id*. at 199-200.

[21] *See* United States v. Wade, 388 U.S. 218, 221-224 (1967).

[22] United States v. Wade, *supra* note 21.

[23] *Id*.

[24] *Id*.; *See* Moore v. Illinois, 434 U.S. 220 (1977).

[25] Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing*, May 2018, pg. 3-4, https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf; *See generally* Madhumita Murgia, *How London Became a Test Case for Using Facial Recognition in* Democracies, The Financial Times, Aug. 1, 2019, https://www.ft.com/content/f4779de6-b1e0-11e9-bec9-fdcab53d6959.

[26] Center on Privacy and Technology, *The Perpetual Lineup: Unregulated Police Face Recognition in America*, Georgetown Law, Oct. 18, 2016, https://www.perpetuallineup.org/.

[27] *Id*.

[28] Stanley, *supra* note 12.

[29] *See* Center on Privacy and Technology, *supra* note 26.

[30] *See Gender Shades*, MIT Media Lab, http://gendershades.org/index.html.

[31] Russell Brandon, *Amazon's Facial Recognition Matched 28 Members of Congress to Criminal Mugshots*, The Verge, July 26, 2018, https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

[32] *Id*.

[33] Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias,* The New York Times, Jul. 8, 2019, https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html.

[34] Steve Lohr, *Facial Recognition is Accurate, if You're a White Guy*, The New York Times, Feb. 9, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[35] *Id*.; Clare Garvie and Jonathan Frankle, *Facial Recognition Software Might Have a Racial Bias Problem*, The Atlantic, Apr. 7, 2016, https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[36] *See* Lohr, *supra* note 34.; *See* Garvie and Frankle, *supra* note 35.; *See generally* Xavier Picket, *Policing Black Communities*, Public Justice Report, First Quarter 2007. Vol. 30. No. 1, https://www.cpjustice.org/uploads/Policing_Black_Communities.pdf; *See also* Jennifer Gonnerman, *Before the Law*, The New Yorker, Oct. 6. 2014, https://www.newyorker.com/magazine%20/2014/10/06/before-the-law (discussing how many individuals from communities of color lack the socioeconomic resources to make bail and are often incarcerated for months – or even years – while awaiting trial, or the dismissal of charges, without ever being convicted of a crime).

[37] Garvie and Frankle, *supra* note 35.; Brian Brackeen, *Facial Recognition Software is Not Ready for Use by Law Enforcement*, TechCrunch, July 2018, https://techcrunch.com/2018/06/25/facial-recognition-software-is-not-ready-for-use-by-law-enforcement/; Lauren Goode, *Facial Recognition Software is Biased Towards White Men,*

Researcher Finds, The Verge, Feb. 11, 2018, https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error.

[38] Chinoy, *supra* note 16.

[39] *Id.*

[40] Center on Privacy and Technology, *supra* note 26.

[41] *Id*.

[42] Harwell, *supra* note 13.

[43] Joseph Goldstein and Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, The New York Times, Aug. 1, 2019, https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

[44] *Id*.

[45] Chinoy, *supra* note 16.

[46] Center on Privacy and Technology, *supra* note 26.

[47] *Id*.

[48] *Id*.

[49] *Id*.

[50] *See* Giorgio Agamben, *No to Bio-Political Tattooing*, from Le Monde, Jan. 10, 2004, https://ratical.org/ratville/CAH/totalControl.pdf.

[51] Id.; Stanley, *supra* note 12; *See* Jay Stanley, *What's Wrong with Airport Face Recognition?*, ACLU, Aug. 4, 2017, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/whats-wrong-airport-face-recognition.

[52] Agamben, *supra* note 50.; Stanley, *supra* note 12.; Stanley, *supra* note 51.

[53] *Id.*; Symanovich, *supra* note 8.

[54] Nadia Kovacs, *What is the Internet of Things*, Norton, https://us.norton.com/internetsecurity-iot-what-is-the-internet-of-things.html.

[55] Maddie Stone, *These Glasses Block Facial Recognition Technology*, Gizmodo, Aug. 8, 2015, https://gizmodo.com/these-glasses-block-facial-recognition-technology-1722826081; *See* Robinson Meyer, *Anti-Surveillance Camouflage for Your Face*, The Atlantic, Jul. 24, 2014, https://www.theatlantic.com/technology/archive/2014/07/makeup/374929/.

[56] Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, The New York Times, Jul. 13, 2019, https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

[57] *Id.*

[58] *Id.*; Maria Korolov, *What is Biometrics? And Why Collecting Biometric Data is Risky*, CSO, Feb. 12, 2019, https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html; *See* James A. Martin, *5 Things to Know About Fitness Tracker and Security in 2018*, CSO, Jul. 5, 2018, https://www.csoonline.com/article/3286214/5-things-to-know-about-fitness-trackers-and-security-in-2018.html; *See also*, Zak Doffman, *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report*, Forbes, Aug. 14, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#70270f9246c6.

[59] Jonathan Kent, *Malaysia Car Thieves Steal Finger*, BBC News, Mar. 31, 2005, http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.

[60] Drew Harwell, *A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job*, The Washington Post, Oct. 25, 2019, https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

[61] *Id.*

[62] Alison Knezevich and Kevin Rector, *Social Media Companies Rescind Access to Geofeedia, Which Fed Information to Police During 2015 Unrest*, The Baltimore Sun, Oct. 11, 2016, https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html; Alvaro Beydoa, *Who's Logging Your Face?*, The Washington Post, Mar. 22, 2017, https://www.washingtonpost.com/opinions/whos-logging-your-face/2017/03/22/47d96142-0e67-11e7-ab07-07d9f521f6b5_story.html?utm_term=.bac654b1913c.

[63] Center on Privacy and Technology, *supra* note 26.

[64] Symanovich, *supra* note 8.

[65] *See* Kyllo v. United States, 533 U.S. 27 (2001).; *See* United States v. Jones, 565 U.S. 400 (2012).; *See* Riley v. California, 573 U.S. 373 (2014).; *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).; *See* Robyn Greene and Michael Pizzi, *The Supreme Court Made a Sweeping Decision About Privacy Rights*, New America, Jul. 26, 2018, https://www.newamerica.org/weekly/supreme-court-made-sweeping-decision-about-privacy-rights/ (discussing how "Carpenter also raises more questions about how law enforcement should handle the surveillance of other data created or stored online. The Electronic Communications Privacy Act of 1986 does not require the government to get a warrant to collect the contents of your online communications that are over 180 days old. Further, the government claims that your web browsing history doesn't constitute communications contents, and thus is not subject to a warrant requirement, so long as it doesn't collect the data after the slash. In other words, the government asserts that it does not need a warrant to learn that you visited www.plannedparenthood.com, but it would need a warrant to learn that you visited its 'learn more: abortion' page. In the government's view, your contacts, buddy lists, and communication logs are also not protected by a warrant requirement. And the list goes on. Whether its data created by Internet of Things devices like Amazon Alexa and smart television sets or DNA databases held by companies like 23andMe or Ancestry.com, Carpenter leaves many other types of personal data in legal limbo.").; *See also* Maynard v. United States, 615 F.3d 544, 562-568 (D.C. Cir. 2010) (discussing the Mosaic Theory, which views collective government surveillance to constitute a search under the Fourth Amendment as it can reveal more about an individual's actions than one single or short terms observation).

[66] Tom Simonite, *Facebook Creates Software That Matches Faces Almost as Well as You Do,* MIT Technology Review, Mar. 17, 2014, https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/; *See generally*, *Technology – Deep Learning*, Herta, https://www.hertasecurity.com/en/technology.

[67] The Biometric Information Privacy Act (BIPA) requires that entities obtain affirmative consent from individuals before obtaining their biometric information and creates a private right of action for individuals to sue to enforce the law. BIPA and other state and federal laws and regulations are discussed in more detail in Section VI of this report "Legislation and Regulations Dealing with Facial Recognition Software and Biometrics" starting on pg. 14.

[68] Dana Herra, *Judge Tosses Illinois Privacy Law Class Action vs Facebook Over Photo Tagging,* The Cook County Record, Jan. 27, 2016, https://cookcountyrecord.com/stories/510660138-judge-tosses-illinois-privacy-law-class-action-vs-facebook-over-photo-tagging-california-cases-still-pending.

[69] In re Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535, (N.D. Cal. 2018).

[70] Jennifer Lynch and Adam Schwartz, *Victory! Illinois Supreme Court Protects Biometric Privacy,* Electronic Frontier Foundation, Jan.25, 2019, https://www.eff.org/deeplinks/2019/01/victory-illinois-supreme-court-protects-biometric-privacy.

[71] *See generally*, Josh Constine, *$350B Face Data Lawsuit Against Facebook Will Proceed*, TechCrunch, Oct. 18, 2019, https://techcrunch.com/2019/10/18/facebook-35-billion-lawsuit/.

[72] Nicholas Iovino, *Facebook Fights $30 Billion Privacy Suit at Ninth Circuit,* Courthouse News Service, Jun. 12, 2019, https://www.courthousenews.com/facebook-fights-30-billion-privacy-suit-at-ninth-circuit/; Patel v. Facebook, Inc., 932 F.3d 1264, 1270 (9th Cir. 2019).; Friends of Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U.S. 167, 180-181 (2000) (discussing how the Case or Controversy clause of Article III of the U.S. Constitution requires that a plaintiff has suffered "(1) an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical, (2) the injury must be fairly traceable to the challenged action of the defendant, and (3) it must be likely, as opposed to merely speculative, that this injury will be redressed by a favorable decision.").

[73] *Id*. at 1270-1273.

[74] Id. at 1273 (quoting Riley v. California, 573 U.S. 373 at 393 (2014) ("Technological advances provide 'access to a category of information otherwise unknowable,' and 'implicate privacy concerns' in a manner as different from traditional intrusions as 'a ride on horseback' is different from 'a flight to the moon . . .'").).

[75] Shannon Liao, *Facebook Hit with Four Lawsuits in One Week Over Cambridge Analytica Scandal*, The Verge, Mar. 23, 2018, https://www.theverge.com/2018/3/23/17155754/facebook-cambridge-analytica-data-breach-scandal.

[76] Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian, Mar. 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[77] *See* Ken Winterbottom, *Court Rules Police ay Compel Suspects to Unlock Fingerprint-Protected Smartphones*, Harvard Journal of Law & Technology, Nov. 12, 2014, https://jolt.law.harvard.edu/digest/court-rules-police-may-compel-suspects-to-unlock-fingerprint-protected-smartphones; *See* Jeff Welty, *Facial Recognition, Biometric Identification and the Fifth Amendment*, North Carolina Criminal Law Blog, (Sept. 18, 2017, 9:25 AM), https://nccriminallaw.sog.unc.edu/facial-recognition-biometric-identification-fifth-amendment/; *See* Bryanna Gutierrez, *Is Your Fingerprint the Golden Ticket for Police?*, Ristenpart Law, Apr. 13, 2017, https://ristenpartlaw.com/case-law-updates-posts/2017/4/11/protecting-fingerprint-scanning-against-unlocking-phones.

[78] *See* Matt Hamilton, *The Government Wants Your Fingerprint to Unlock Your Phone. Should That be Allowed?*, Apr. 30, 2016, The Los Angeles Times, https://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html.

[79] Matter of Residence in Oakland, California, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019); *See* Thomas Brewster, *Feds Can't Force You to Unlock Your iPhone With Finger or Face, Judge Rules*, Forbes, Jan. 14. 2019, https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules/#7323bbf042b7.

[80] *Id*. at 1016-1017.

[81] In re Application for a Search Warrant, 236 F. Supp. 3d 1066, (N.D. Ill. 2017).

[82] *Id*. at 1068-1069.

[83] *Id*. at 1071 (citing Fisher v. United States, 425 U.S. 391, 410 (1976).

[84] In re Application for a Search Warrant, *supra* note 81 at 1074.

[85] Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case, No. 1:19-MJ-10441-DCN, 2019 WL 3401990, at 1 (D. Idaho July 26, 2019).

[86] *Id*. at 4.

[87] *Id*. at 7.

[88] Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014).

[89] *Id*. at 3 (citing United States v. Kirschner, 823 F.Supp.2d 665, 669 (E.D.Mich.2010)).

[90] Commonwealth v. Baust, *supra* note 88 at 3.; United States v. Wade, *supra* note 21 at 223.

[91] *Id*.; *See* Welty, *supra* note 77.

[92] State v. Diamond, 890 N.W.2d 143, 145 (Minn. Ct. App. 2017).

[93] *Id*. at 150-151.

[94] Florida v. Stahl, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016).

[95] Nathan Freed Wessler and Somil Trivedi, *Florida is Using Facial Recognition to Convict People Without Giving Them a Chance to Challenge the Technology*, ACLU, 2019, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/florida-using-facial-recognition-convict-people; Aaron Mak, *Facing Facts*,

Slate, Jan. 25, 2019, https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html.

[96] *Id*. (discussing how during a deposition of the Jacksonville crime analyst who used FACES to obtain a "one star" match of the defendant, the crime analyst testified that FACES rates the quality of a match using a star system and that while the defendant had a one-star match, other potential matches had none. The analyst also did not know the maximum number of stars possible for a FACES match).

[97] Karen Gullo and Jennifer Lynch, *When Facial Recognition Is Used to Identify Defendants, They Have a Right to Obtain Information About the Algorithms Used on Them, EFF Tells Court*, Electronic Frontier Foundation, Mar. 12, 2019, https://www.eff.org/deeplinks/2019/03/when-facial-recognition-used-identify-defendants-they-have-right-obtain; *See* Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018).

[98] Russell Brandom, *Facebook-backed Lawmakers are Looking to Gut Privacy Law*, The Verge, Apr. 10, 2018, https://www.theverge.com/2018/4/10/17218756/facebook-biometric-privacy-lobbying-bipa-illinois; Russell Brandom, *Crucial Biometric Privacy Law Survives Court Fight*, The Verge, Jan. 26, 2019 https://www.theverge.com/2019/1/26/18197567/six-flags-illinois-biometric-information-privacy-act-facial-recognition.

[99] *See* Rosenbach v. Six Flags, 2019 IL 123186 (Jan. 25, 2019).

[100] *Id*. at 38-39; Brandom, *supra* note 98.

[101] *Id*.

[102] Thomas F. Brier Jr. and Jeffrey N. Rosenthal, *Biometrics and the New Wave of Class Action Lawsuits*, The Legal Intelligence Mar. 1, 2019, https://www.law.com/thelegalintelligencer/2019/03/01/biometrics-and-the-new-wave-of-class-action-lawsuits/; *See* Jeffrey D. Neuburger, *Wow! Illinois Biometric Privacy Suits Proliferate*, The National Law Review, Sept. 27, 2017, https://www.natlawreview.com/article/wow-illinois-biometric-privacy-suits-proliferate; *See* Chris Burt, *EEF Urges Appeals Court to Side with Plaintiff Interpretation of Harm in Facebook Biometric Privacy Suit*, Biometric Update, Dec. 18, 2018, https://www.biometricupdate.com/201812/eff-urges-appeals-court-to-side-with-plaintiff-interpretation-of-harm-in-facebook-biometric-privacy-suit.

[103] *Id*.

[104] People v. Weaver, 12 N.Y.3d 433 (2009).

[105] *See* State v. Andrews, 457 N.J. Super. 14, 22-24 (App. Div. 2018) (discussing how if the government already knows that a defendant has a password to a device, then compelling the defendant to produce the password is not considered a testimonial act and thus not violate of the Fifth Amendment. Specifically, this occurs when (1) the Government has knowledge of the evidence, (2) the defendant possessed or controlled the evidence and (3) the evidence is authentic. In this case, the information provided by the defendant would be a "foregone conclusion.").

[106] *Id*. at 34; Commonwealth v. Baust, *supra* note 88.

[107] Thakkar, *supra* note 10.

[108] *Electronic Communications Privacy Act Primer*, cdt, May 13, 2015, https://cdt.org/insight/electronic-communications-privacy-act-primer/.

[109] *Electronic Communications Privacy Act Primer*, *supra* note 109.

[110] *Id*.

[111] 18 U.S.C. § 2703(d) (West).

[112] S.847 – 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/847/text.

[113] S.2968 – 116th Congress (2019-2020, https://www.congress.gov/bill/116th-congress/senate-bill/2968; *Consumer Online Privacy Rights Act of 2019*, Maria Cantwell United States Senator for Washington, https://www.cantwell.senate.gov/imo/media/doc/COPRA%20One-Pager.pdf.; Cantwell, Senate Democrats Unveil Strong Online Privacy Rights, 2019, https://www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights; Tony Romm, *Top Senate Democrats Unveil New Online Privacy Bill, Promising Tough Penalties for Data Abuse*, The Washington Post, Nov. 26, 2019, https://www.washingtonpost.com/technology/2019/11/26/top-senate-democrats-unveil-new-online-privacy-bill-promising-tough-penalties-data-abuse/.

[114] *Id*.

[115] *Id*.

[116] H.R. 4008 – 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/4008?s=1&r=7.

[117] *See* Todd Spangler, *Rep. Rashida Tlaib Sponsors Bill Cracking Down on Use of Facial Recognition Technology*, Detroit Free Press, Jul. 25, 2019, https://www.freep.com/story/news/local/michigan/2019/07/25/rep-rashida-tlaib-cracking-down-facial-recognition-technology/1824706001/; Harmon, *supra* note 33.

[118] S.1933 – 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/1933; H.R. 3377 – 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/3377/text?r=2&s=2.

[119] *Id*.

[120] *Id*.

[121] *Id*.

[122] *See*, H.R. 4008, *supra* note 116.

[123] National Institute of Standards and Technology (NIST), Face Recognition Vendor Test, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt; *See generally*, NIST, Topics, https://www.nist.gov/topics.

[124] NIST, Face Recognition Vendor Test – Ongoing, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing.

[125] *See* Kenn Brotman & Molly K. McGinley, *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, The National Law Review, Mar. 25, 2019, https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states.

[126] *Id*.

[127] *Several States Consider Laws Regulating the Collection of Biometric Data*, Lexology, Feb. 6, 2019, https://www.lexology.com/library/detail.aspx?g=a545aec6-37b8-49a8-8487-74b61883a0e1.

[128] 740 Ill. Comp. Stat. 14 (2008).

[129] Daniel Healow, Stuart D. Levi, Brian O'Connor, William Ridgway and James S. Talbot, , *Illinois Supreme Court Holds that Biometric Privacy Law Does Not Require Actual Harm for Private Suite,* Skadden, Jan. 29, 2019, https://www.skadden.com/insights/publications/2019/01/illinois-supreme-court.

[130] 740 Ill. Comp. Stat., *supra* note 128 at 14/10 & 15.

[131] 740 Ill. Comp. Stat., *supra* note 128 at 14/20(1).

[132] *Id*. at 14/20(2).

[133] *Id*. at 14/20(3).

[134] Tex. Bus. & Com. Code Ann. § 503.001 (West 2019).

[135] *Id*.

[136] Brotman & McGinley, *supra* note 126.

[137] Wash. Legis. Serv. Ch. 299 (S.H.B. 1493) (West).

[138] *Id*.

[139] *See* Bill Information, SB 5376-2019-20, Washington State Legislature, https://app.leg.wa.gov/billsummary?BillNumber=5376&Year=2019&Initiative=false.

[140] *Id*.

[141] *Id*.

[142] *See* HB 1071 - 2019-20 – Bill Information, Washington State Legislature, https://app.leg.wa.gov/billsummary?BillNumber=1071&Year=2019.

[143] *Id*; *See also*, *Washington's New Data Breach Law Follow Enhanced Privacy Protection* Trends, Thompson Hine, May 20, 2019, https://www.thompsonhine.com/publications/washingtons-new-data-breach-law-follows-enhanced-privacy-protection-trends.

[144] HB 1071, Washington State Legislature, http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Passed%20Legislature/1071-S.PL.pdf (*see* specifically Sec. 1.(2)(a)(i)(I)).

[145] *Id*. at Sec. 2.(1) and (7).

[146] HB 1071, *supra* note 144 at Sec. 5.(7).

[147] *Id*. at Sec. 2.(1).

[148] *Id* at Sec. 1.(2).

[149] Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, Wired, Jun. 28, 2018, https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/.

[150] Cal. Civ. Code § 1798.100 **(**West 2018).

[151] Lapowsky, *supra* note 149.

[152] Cal. Civ. Code, *supra* note 150.

[153] *Id*.

[154] *Id*.

[155] Lapowski, *supra* note 149; *See* JD *Amendments to California Consumer Privacy Act Head to Governor's Desk*, Supra, Sept. 6, 2018, https://www.jdsupra.com/legalnews/amendments-to-california-consumer-92796/.

[156] A.1911/S.1203, *supra* note 156.

[157] *Id*.

[158] A.1911/S.1203, 243rd Session (N.Y 2019), https://www.nysenate.gov/legislation/bills/2019/s1203 (introduced in 2018 at A.9793/S.8547).

[159] *NetChoice's Internet Advocates' Watchlist for Ugly Laws (iAWFUL) Targets Worst Bills and Laws for Online Consumers and Entrepreneurs*, April 4, 2018, NetChoice, https://netchoice.org/media-press/the-iawful-7-state-federal-and-international-legislation-placing-barriers-to-innovation-and-commerce/ (last visited Aug. 7, 2020).

[160] *See* 2019 N.Y. Laws ch. 117, *available at* https://www.nysenate.gov/legislation/bills/2019/s5575; N.Y. LAB. Law § 201-a (McKinney 2019).

[161] Annemaria Duran, *New York Employers Can Eliminate Buddy Punching With Biometric Time Clocks*, Swipeclock, Jan. 8, 2018, https://www3.swipeclock.com/blog/new-york-employers-can-eliminate-buddy-punching-biometric-time-clocks/.

[162] Chp. 117, *supra* note 158; *See New York SHEILD Act Expands Privacy and Cybersecurity Obligations*, Thompson Hine, Jul. 29, 2019, https://www.thompsonhine.com/publications/new-york-shield-act-expands-privacy-and-cybersecurity-obligations.

[163] Chp. 117, *supra* note 158.

[164] *Id*.

[165] *Id*.

[166] A.7790/S.5687, 243rd Session (N.Y. 2019), https://www.nysenate.gov/legislation/bills/2019/s5687.

[167] Elizabeth Elizalde and Michael Gartland, *Brooklyn Tenants in Rent-Regulated Apartments Push State to Nix Landlord's facial Recognition Software*, Daily News, May, 1, 2019, https://www.nydailynews.com/new-york/brooklyn/ny-facial-recognition-brownsville-nelson-20190501-5gb32fncjrcmvijwbriimwpcsa-story.html.

[168] *Id*.

[169] Some of this proposed legislation includes: A.235/S.2500 – Relates to the use of biometric data for marketing purposes; A.465 – Enacts the "personal information protection act"; A.1911/S.1203 – Establishes the biometric privacy act; A.2114 – Relates to identity theft; clarifies personal identifying information and what acts constitute the offense of identity theft; A.2614 – Establishes a driver safety course and a driver safety course fund; A.2830 – Establishes the Medicaid identification and anti-fraud biometric technology pilot program appropriation; A04030 – Regulates the use of unmanned aerial vehicles by the state and political subdivisions thereof; A.4076-B/S.4352-B – Relates to providing for electronic notarization; A.4299 – Relates to unlawfully purchasing or selling personal identifying information; A.5635-B/S.5575-B – Relates to a notification of a security breach; A.5757 – Relates to the use of biometric identity verification devices for the purchase of alcoholic beverages and tobacco products; A.6351/S.4411 – Allows consumers the right to request from businesses the categories of personal information a business has sold or disclosed to third parties; A.6787-D/S.5140-B – Relates to the use of biometric identifying technology; A.6788-B/S.5125-B – Relates to limitations on smart access systems for entry; A.7613/S.7724 – Relates to establishing the New York Data Protection Act; A.7736 – Establishes the "It's Your Data Act"; A.7913/S.5222 – Relates to the crimes of commercial bribery and larceny; A.8169 – Relates to protecting personal information; A.8526/S.5642 – Relates to enacting the NY privacy act; S.1749 – Relates to creating a private right of action for the breach of a consumer's identifying information; A.10725/S.1844 – Establishes and redefines offenses involving fraud, scheme to defraud and larceny; S.5146 – Relates to offenses involving thefts of identity; S.6007 – Relates to the use of biometric identity verification devices for the purchase of alcoholic beverages and tobacco products; S.6776 – Relates to prohibiting facial recognition technology to be used in connection with an officer camera; A.1692 – Prohibits the state, state agencies and departments and contractors doing business with the state, its agencies or departments from retaining facial recognition images; A.4030 – Regulates the use of unmanned aerial vehicles by the state and political subdivisions thereof; A.7790/S.5687 – Prohibits the use of a facial recognition system by a landlord on any residential premises; A.8042/S.6623 – Enacts the "facial recognition technology study act; A.8373 – Prohibits the use of a facial recognition system by any person on public school premises; A.9931-A/S.6435-B – Imposes limitations on the use of drones for law enforcement purposes; S.6776 – Relates to prohibiting facial recognition technology to be used in connection with an officer camera. Relevant bill text can be accessed through https://www.nysenate.gov/search/legislation.

[170] A.9767/S.7572, 243rd Session (N.Y 2020), https://www.nysenate.gov/legislation/bills/2019/s7572.

[171] *Id*.

[172] *See* The New York State Assembly, *supra* note 169.

[173] HB 1943, Arkansas State Legislature, http://www.arkleg.state.ar.us/assembly/2019/2019R/Bills/HB1943.pdf.

[174] *Id*.

[175] Katie Lannan, *Sommerville Bans Government Use of Facial Recognition Technology*, wbur, Jun. 28, 2019, https://www.wbur.org/bostonomix/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech.

[176] Kate Conger, Richard Fausset and Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, The New York Times, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html; *See* Harwell, *supra* note 13.

[177] *Id*.; Harwell, *supra* note 13.; Rachel Metz, *Beyond San Francisco, More Cities Are Saying No To Facial Recognition*, CNN Business, Jul. 17, 2019, https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

[178] *Id*.

[179] Sarah Wu, *Sommerville City Council Passes Facial Recognition Ban,* The Boston Globe, https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html.

[180] Tom McKay, *Berkeley Becomes the Fourth U.S. City to Ban Face Recognition in Unanimous Vote*, Gizmodo, Oct. 16, 2019, https://www.msn.com/en-us/news/technology/berkeley-becomes-fourth-us-city-to-ban-face-recognition-in-unanimous-vote/ar-AAIRKiD.

[181] Local Law No. 65 (2020) of City of New York, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0&Options=ID|Text|&Search=0487. .

[182] *Id*.

[183] *Id*.

[184] *See* Council of City of NY Int. 1170-2018, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3704369&GUID=070402C0-43F0-47AE-AA6E-DEF06CDF702A&Options=&Search=.

[185] *Id*. (describing how Int. 1170-2018 defines "biometric identifier information" as ". . . a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, any of which is collected, retained, converted, stored or shared to identify an individual." The Bill also requires (1) businesses to provide conspicuous notice that biometric data is being collected and (2) make available online, "1. The amount of time for which the commercial establishment retains or stores biometric identifier information; 2. The kind of biometric identifier information the commercial establishment collects, retains, converts, stores or shares from its customers; 3. Any privacy policy governing, and any purpose for, the commercial establishment's collection, retention, conversion, storage or sharing of biometric identifier information of customers, including but not limited to, any protective measures the commercial establishment utilizes to safeguard biometric identifier information; and 4. Whether the commercial establishment shares biometric identifier information with third-parties.").

[186] Int. 1170-2018, *supra* note 184.

[187] *Id*.

[188] *Id*.

[189] *Id*.

[190] Stephanie Kapinos, *New York City Considers Facial Recognition Bill – Will New York Be the Next Forum for Biometric Privacy Litigation?,* Proskauer – New Media and Technology Law Blog, Jan. 31, 2019, https://newmedialaw.proskauer.com/2019/01/31/new-york-city-considers-facial-recognition-bill-will-new-york-be-the-next-forum-for-biometric-privacy-litigation/.

[191] *See* Council of City of NY Int. 1758-2019, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4085862&GUID=1D415200-95B9-440B-AE2B-F0B5F9668B0A&Options=&Search=.

[192] *Id*.

[193] *Id*.

[194] *See* Council of City of NY Int. 1672-2018, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4146261&GUID=435ECCD7-D2E0-4029-AEB2-3167FB9F6714&Options=&Search=.

[195] *Id*.

[196] *See 2018 Reform of EU Data Protection Rules*, European Commission, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#abouttheregulationanddataprotection.

[197] *Id*.

[198] Regulation 2016/679, Art. 1, 2016 O.J. (L 127) (EU).

[199] *Id*. at Art. 4, 1.

[200] *See* Data Protection Act, 2018, c. 12 (U.K.).

[201] Big Brother Watch, *supra*, note 25 at 47.

[202] Madhunita Murgia, *London Could Shape the Future of Facial Recognition*, OZY, Aug. 5, 2019, https://www.ozy.com/fast-forward/london-could-shape-the-future-of-facial-recognition/95951/.

[203] *Id*.

[204] James Vincent, *The Tech Industry Doesn't Have a Plan for Dealing with Facial Bias*, The Verge, Jul. 26, 2018, https://www.theverge.com/2018/7/26/17616290/facial-recognition-ai-bias-benchmark-test; Stephen Mayhew, *Police in China Using Facial Recognition Glasses*, Biometric Update, Feb. 7, 2018, https://www.biometricupdate.com/201802/police-in-china-using-facial-recognition-glasses.

[205] *Chinese Facial Recognition Tech Installed in Nations Vulnerable to Abuse*, CBS News, Oct. 16, 2019, https://www.cbsnews.com/news/china-huawei-face-recognition-cameras-serbia-other-countries-questionable-human-rights-2019-10-16/.

[206] *Id*.

[207] *Id*.

[208] *Chinese Facial Recognition Tech Installed in Nations Vulnerable to Abuse*, *supra* note 206.

[209] Id.; *See also*, Sharon Weinberger, *Private Surveillance Is a Lethal Weapon Anyone Can Buy*, The New York Times, Jul. 19, 2019, https://www.nytimes.com/2019/07/19/opinion/private-surveillance-industry.html?action=click&module=Opinion&pgtype=Homepage (discussing how large American tech companies and defense contractors have also sold biometric surveillance tools to foreign governments for purposes of spying on their citizens and instituting human rights violations; the selling of biometric surveillance technology to governments has become a multibillion-dollar industry.).

[210] *See generally*, *About UIDAI*, Unique Identification Authority of India, https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html.

[211] Id.; *See* The Aadhaaar (Targeted Delivery of Financial And Other Subsidies, Benefits and Services) Act, No. 18 of 2016.

[212] Reetika Khera, *These Digital IDs Have Cost People Their Privacy – and their Lives*, The Washington Post, Aug. 9, 2018, https://www.washingtonpost.com/news/theworldpost/wp/2018/08/09/aadhaar/?utm_term=.6273ab2e1fcc; *See* Pranav Rai, *The Indian Supreme Court's Aadhaar Judgement – A Privacy Analysis*, IAPP, Oct. 9, 2018, https://iapp.org/news/a/the-indian-supreme-courts-aadhaar-judgement-a-privacy-perspective/.

[213] Woodrow Hartzog and Evan Selinger, *Facial Recognition is the Perfect Tool for Oppression*, The Medium, 2017, https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66; Woodrow Hartzog & Evan Selinger, *Why We Must Ban Facial Recognition Software Now*, The New York Times, Oct. 17. 2019, https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html; *See* Evan Greer, *Opinion: Don't Regulate Facial Recognition. Ban It.*, BuzzFeed, Jul. 18, 2019, https://www.buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it.

[214] Hartzog and Evan Selinger, *supra* note 214.; Hartzog and Evan Selinger, *supra* note 214.; Greer, *supra* note 214.

[215] Anna Parsons, *Why a Blanket Ban of Facial Recognition Technology Would be Bad Policy*, The Hill, Sept. 16. 2019, https://thehill.com/blogs/congress-blog/technology/461618-why-a-blanket-ban-of-facial-recognition-technology-in-schools.

[216] Vincent, *supra* note 205.; James Vincent, *IBM Hopes to Fight Bias in Facial Recognition with New Diverse Dataset*, The Verge, Jun. 27, 2018, https://www.theverge.com/2018/6/27/17509400/facial-recognition-bias-ibm-data-training.

[217] *See generally*, FATE - Fairness Accountability, Transparency and Ethics in AI, Microsoft, https://www.microsoft.com/en-us/research/group/fate/ (one example of a company making efforts to combat bias in its biometric software).

[218] Nick Statt, *Amazon Told Employees it Would Continue to Sell Facial Recognition Software to Law Enforcement*, The Verge, Nov. 11, 2018, https://www.theverge.com/2018/11/8/18077292/amazon-rekognition-jeff-bezos-andrew-jassy-facial-recognition-ice-rights-violations.

[219] *Id*.

[220] Michael Punke, *Some Thoughts on Facial Recognition Legislation,* AWS Machine Learning Blog (Feb. 7, 2019) https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/.

[221] Nick Statt and James Vincent, *Google Pledges Not to Develop AI Weapons, but Says it Will Still Work with the Military*, The Verge, Jun. 7, 2019, https://www.theverge.com/2018/6/7/17439310/google-ai-ethics-principles-warfare-weapons-military-project-maven; *Artificial Intelligence at Google – Our Principals,* Google, https://ai.google/principles.

[222] *Id*.

[223] IIIE, *Ethics in Action*, https://ethicsinaction.ieee.org/.

[224] *See generally* Algorithmic Justice League, https://www.ajlunited.org/.

[225] Kevin McCarthy, *Don't Count on Governments to Protect Your Privacy,* The New York Times, Jul. 14, 2019, https://www.nytimes.com/2019/07/14/opinion/kevin-mccarthy-privacy-blockchain.html.

[226] Id.

[227] *See generally,* Karen Weise and Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, The New York Times, Jun. 10, 2020, https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html?auth=login-email&login=email; Hannah Klein, *IBM Says It Will Stop Developing Facial Recognition Tech Due to Racial Bias,* Slate, Jun. 9, 2020, https://slate.com/technology/2020/06/ibm-facial-recognition-racial-bias.html; Nathan Sheard, *Victory! New York's City Council Passes the POST Act,* Electronic Frontier Foundation, Jun. 18, 2020, https://www.eff.org/deeplinks/2020/06/victory-new-yorks-city-council-passes-post-act. (In the wake of worldwide protests stemming from the May 2020 killing of George Floyd - an unarmed African American man who died of asphyxiation after a Minneapolis police officer refused to remove his knee from Mr. Floyd's neck as he lay face down in handcuffs repeatedly pleading "I can't breathe" - several private sector companies, including Amazon and IBM, publicly stated that they would halt their development of facial recognition software due to concerns over racial bias and the use of their software by law enforcement. Relatedly, some municipalities have recently passed laws regulating law enforcement's use of personal data: just weeks after George Floyd's killing, the New York City Council passed the POST Act (*see supra* note 181). We must continue to build on the momentum of this moment and craft comprehensive legislative and policy reforms aimed at eradicating racial bias from facial recognition and other biometric technology).

[228] Vincent, *supra* note 205.

[229] *See* Angela Chen, *How to Kick Facial Recognition Out of Your Town*, MIT Technology Review, Oct. 4, 2019, https://www.technologyreview.com/s/614477/facial-recognition-law-enforcement-surveillance-private-industry-regulation-ban-backlash/.