Journal of Business & Technology Law

Volume 15 | Issue 2 Article 7

Facial Recognition Technology: Balancing the Benefits and Concerns

Elizabeth McClellan

Facial Recognition Technology: Balancing the Benefits and Concerns

ELIZABETH MCCLELLAN* ©

INTRODUCTION

Facial recognition technology is becoming increasingly prevalent in today's world. From airports,[1] to apps on your phone,[2] to even your local supermarket,[3] technology is seemingly tracking faces at all times. However, what is "facial recognition technology," and how does it work?

Facial recognition technology is an algorithm used to recognize a human face through the use of biometrics, which track facial features from a photo or video.[4] These facial features often include the distance between your eyes, the distance from your forehead to your chin, and other "facial landmarks"—thus creating your "facial signature."[5] Facial recognition technology is used by governmental agencies, as well as private corporations. For example, the Department of Homeland Security has used facial recognition technology in several airports to help identify individuals who may be under criminal investigation, or who have overstayed their visas.[6] In August of 2018, just days after installing the facial recognition technology, U.S. Customs and Border Protection at Washington Dulles International Airport was able

* J.D. Candidate, 2021, University of Maryland Francis King Carey School of Law. The author would like to thank the editors and staff on the Journal of Business & Technology Law for their feedback and support throughout the writing process. The author would also like to thank her family and friends, and especially Jonathan McClellan, Loretta McClellan, and Kathleen McClellan, for their continued love, support, and encouragement, without which this paper would not be possible.

1. Stephen Sapp, *CBP at Washington Dulles International Airport Intercepted an Imposter Using new cutting-edge Facial Comparison Biometrics technology*, U.S. CUSTOMS AND BORDER PROTECTION (Aug. 23, 2018) https://www.cbp.gov/newsroom/local-media-release/cbp-washington-dulles-international-airport-intercepted-imposter-using.

2. *About Face ID advanced technology*, APPLE, https://support.apple.com/en-us/HT208108 (last visited Apr. 4, 2020).

3. Tom Chivers, *Facial Recognition…Coming to a Supermarket Near you*, THE GUARDIAN (Aug. 4, 2019), https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties.

4. Steve Symanovich, *How Does Facial Recognition Work?*, NORTON, https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html (last visited Apr. 4, 2020).

5. *Id.*

6. *Supra* note 1.

to identify and arrest an imposter attempting to enter the United States—the facial recognition software identified the individual's face, and recognized that his face was not a match to the passport he presented.[7]

Facial recognition technology is also utilized by social media companies and private corporations, including Apple. In 2017, Apple announced the use of their new "Face ID" feature on iPhones. Face ID "accurately map[s] the geometry of your face" by "projecting and analyzing over 30,000 invisible dots to create a depth map of your face and…capture[] an infrared image of your face."[8] Face ID allows one to unlock their Apple device, authorize purchases made on the device, and sign into apps downloaded on the device.[9] Apple claims there is a 1 in 1,000,000 probability that a random person may look at another person's device and unlock it using Face ID.[10]

Social media sites such as Facebook similarly utilize facial recognition technology by analyzing photos the website's users are identified in, including profile pictures and photos and videos the user has been tagged in, to create a "template" for every user.[11] This "template" is then used to identify photos and videos of the user's face, as well as protect users from impersonation and identity misuse by detecting if a user appears in someone else's profile picture.[12]

The use of facial recognition technology has continued to grow and expand, providing helpful and creative uses in almost all aspects of life. The expansive use of the technology in social media, in particular, has begun to facilitate conversation amongst not only lawmakers, but everyday citizens as well. Although fairly new and exciting to some, facial recognition technology has become increasingly worrisome for many, in part due to the lack of regulations surrounding the technology. As facial recognition technology evolves and expands, there is an increasing need for regulation at the federal level. These regulations should consider and incorporate language that will allow the technology to continue providing benefits to society, but also ensure that limitations and penalties are placed on users of the technology to protect citizens.

This paper will consider the benefits of the technology as well as the concerns that surround the technology to ultimately propose regulations that help balance these interests. Section I will discuss the current laws and regulations surrounding facial recognition technology in the public sector as well as regulations promulgated by private corporations. Section II will discuss the benefits of the technology in light

7. *Id.*

8. *Supra* note 2.

9. *Id.*

10. *Id.*

11. *What is the face recognition setting on Facebook and how does it work?*, FACEBOOK, https://www.facebook.com/help/122175507864081 (last visited Apr. 4, 2020).

12. *Id.*

of current events and uses, and Section III will discuss the concerns of the technology in a similar light. Lastly, Section IV will balance these benefits and concerns to ultimately propose guidelines for potential regulations regarding facial recognition technology, while considering accountability, transparency, and privacy.

I. CURRENT LAWS & REGULATIONS

A. United States Law

In the United States, there are currently no federal statutes regulating facial recognition technology. While there are several state and local ordinances discussing biometrics and surveillance technology, none of the regulations in place directly address facial recognition technology, and the regulations tend to apply very broadly.

Illinois passed the Biometric Information Privacy Act in 2008, which sets forth broad regulations regarding the collection of biometrics in order to protect the public "welfare, security, and safety."[13] These regulations include obtaining consent from citizens, and requiring private entities that collect biometric information to develop and publicize a written policy establishing their guidelines for obtaining, retaining, and destroying these biometric identifiers.[14] Under the statute, citizens are able to recover damages if a business obtains a citizen's biometric information, including fingerprints and facial geometry scans, without the citizen's consent.[15]

Rosenbach v. Six Flags Entertainment Corporation illustrates the breadth of the Illinois statute and the potential issues left unresolved despite the regulation.[16] In Rosenbach, the Illinois Supreme Court held that Six Flags violated the Illinois statute when it required the plaintiff's fingerprint to obtain a season pass without providing a policy describing how the fingerprint would be used or stored.[17] The court further held that an individual could bring a suit under the statute even if the only "harm" suffered was a violation of their legal right under the statute.[18] However, it

13. 740 ILL. COMP. STAT. 14/5 (2008). The statute also notes that "biometric identifier" includes a "scan of hand or face geometry." *Id.* 14/10.

14. *Id.* 14/15.

15. *Id.* 14/20. *See also*, Stuart D. Levi et al., *Illinois Supreme Court Holds That Biometric Privacy Law Does Not Require Actual Harm for Private Suits*, SKADDEN, ARPS, SLATE MEAGHER & FLOM LLP (Jan. 29, 2019), https://www.skadden.com/insights/publications/2019/01/illinois-supreme-court (noting that Texas and Washington are among other states to pass similar legislation, but Illinois remains the only state that allows private individuals to recover damages for a violation of the statute).

16. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197 (Ill. 2019).

17. *Id.* at 1203–04.

18. *Id.* at 1207.

remained unclear whether this harm was enough to provide individuals with constitutional standing in federal court.[19]

The Northern District of Illinois partially addressed this issue in 2018 when it decided Google's "face grouping" feature[20] did not constitute a "concrete injury" to satisfy constitutional standing since there was no substantial risk of harm from Google's collection or retention of the face templates.[21] Conversely, the Ninth Circuit upheld a district court's ruling that users had constitutional standing to sue Facebook for the collection of users' facial images in violation of the Illinois biometrics law, holding that the law protects "concrete privacy interests" and a violation of the law "pose[s] a material risk of harm to those privacy interests."[22] Absent a federal statute or Supreme Court ruling, the question remains unanswered as to exactly what harm is enough to provide standing for cases involving data privacy and facial recognition technology, especially since districts appear to be split on the issue.

The Ninth Circuit's ruling in favor of data privacy does not come as a surprise due to California's increased attention to data privacy.[23] California recently passed legislation that went into effect on January 1, 2020 regulating the privacy of biometric information, as well as personal information.[24] Similar to the Illinois statute, businesses obtaining the information must inform consumers of the information being collected and the purposes of the collection.[25] The California legislation even goes a step further, explicitly stating that consumers have the "right" to request that a business disclose the "specific pieces of personal

19. *Id.* at 1204 (noting that the language of the Illinois Act mirrors the AIDS Confidentiality act, which provides a right of action in a "State circuit court or as a *supplemental claim* in federal district court…" (emphasis added)). The court's opinion did not directly address the issue of constitutional standing, but other courts have been split on the issue. *See infra* notes 20–22 and accompanying text.

20. Through this feature, Google automatically scans all photos uploaded to their apps to identify and group photos of individuals.

21. Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1005 (2018). Although the court held that Google's practices did not constitute a concrete injury, the court did concede that concrete concerns may arise in the future from face-recognition technology, "especially as it becomes more accurate and more widespread." *Id.* at n.15.

22. Patel v. Facebook, Inc., 932 F.3d 1264, 1275 (9th Cir. 2019).

23. California's 2019 legislation follows the 2018 San Francisco Bay Area Rapid Transit District "surveillance ordinance" regulating the use of surveillance technology, recognizing that the technology has many benefits, but should be restricted or limited in order to promote safety and privacy. S.F. BAY AREA RAPID TRANSIT, CAL., ORDINANCE No. 2018-1 (Sept. 21, 2018). The ordinance also appears to significantly value transparency with citizens, requiring that the District release a "Surveillance Annual Report" including a discussion of how the technology is used, how often data is acquired and shared with outside entities, any complaints regarding the technology, and any crime statistics the equipment has deterred or detected. *Id.* This ordinance is particularly interesting since it is seemingly one of the only regulations that regulates a public entity and not merely private companies using the data for "commercial purposes."

24. CAL. CIV. CODE § 1798.100 (2018); CAL. CIV. CODE § 1798.140 (2018) (defining "personal information" as any information related to a household or individual, including biometric information).

25. *Id.*

information" the business has obtained, as well as have the "right" to request that businesses delete any stored personal information about the consumer.[26] As the most innovative and technologically advanced state in the United States, [27] the impact of the California legislation will likely be huge.[28] Many technology companies are located in California, or do significant business in California, and will thus be required to update their privacy policies as a result of these new "rights" given to California citizens.[29]

Along with the California legislation, both Texas and Washington have also passed legislation following the format of the Illinois legislation.[30] Texas and Washington require that a "person" may not capture an individual's "biometric information" for "commercial purposes" without notifying the individual beforehand and obtaining the individual's consent.[31] Despite this similar language, some of the most stark differences come from the definition of "biometric information" and exactly what is protected by these different statutes.

The Texas statute is very narrow, defining biometric information as something that may include only a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.[32] The Illinois statute also defines biometric information similarly to Texas's definition.[33] However, Washington's statute defines biometric information much more broadly: in Washington, biometric information includes the

26. CAL. CIV. CODE § 1798.100 (2018); CAL. CIV. CODE § 1790.105 (2018).

27. Karsten Strauss, *America's Biggest Tech Hubs, By The Jobs*, FORBES (Jul. 26, 2017), https://www.forbes.com/sites/karstenstrauss/2017/07/26/americas-biggest-tech-hubs-by-the-jobs/#567e9a872f15 ("The biggest, most important tech hub…is in San Jose, California…the world's undisputed capital of tech.").

28. 2017 CAL. ADV. LEGIS. SERV. 55 (California's legislature noting that California is one of the "world's leaders in the development of new technologies" and thus must protect the personal information of its consumers). The assembly bill also found that all people "desire privacy and more control over their information" and that thus California consumers should be able to exercise this control. *Id.*

29. *See infra* notes 57–58 and accompanying text.

30. TEX. BUS. & COM. CODE § 503.001 (2009); WASH. REV. CODE § 19.375.020 (2017). Texas also prohibits the person obtaining the biometric information from selling or disclosing the biometric information to another without full disclosure to and consent from the individual, and requires the obtainer to destroy of the information within a "reasonable time," no later than one year after the "date the purpose for collecting the identifier expires." TEX. BUS. & COM. CODE § 503.001 (2009). Washington's law is not as specific, noting that the person possessing the biometric identifier may not retain the information longer than is "reasonably necessary" to comply with a court order or statute, protect against fraud, and "provide the services for which the biometric identifier was enrolled." WASH. REV. CODE § 19.375.020 (2017).

31. TEX. BUS. & COM. CODE § 503.00 (2009)1 ("A person may not capture a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual. . .; and (2) receives the individual's consent. . .); WASH. REV. CODE § 19.375.020 (2017) ("A person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose").

32. TEX. BUS. & COM. CODE § 503.001 (2009).

33. 740 ILL. COMP. STAT. 14/10 (2008).

same information as Texas's statute, but also includes any "unique biological patterns or characteristic used to identify a specific individual."[34] Therefore, information such as health or behavioral data[35] collected on an Apple watch may be collected for commercial purposes under the Texas statute with no protections, but may be protected from collection in the state of Washington.

California's legislation defines biometric information very broadly, perhaps even broader than the Washington and Illinois statutes.[36] Among the listed biometrics defined in the other state statutes, California's definition includes "physiological, biological, and behavioral characteristics" and specifically includes information such as keystrokes and gait patterns, as well as "sleep, health, or exercise data."[37] California's statute seemingly protects all types of data and recognizes the potential changes and developments this data may undergo in the future. The statute also notes that "personal information" may include any information that relates to a household and not just an individual.[38] This is unique to the California statute and will almost certainly spur litigation in order to define what constitutes a "household."

The other most important difference in all the state legislations is the granting of a private right of action. Illinois's Biometric Information Privacy Act remains to be the only legislation that gives individuals a private right of action to sue over breaches of this privacy.[39] Therefore, without a private right of action, and lack of litigation resulting thereof, it is difficult for citizens to illustrate the particular deficits in the state legislation. Despite the fact that there has not been federal legislation or litigation regarding biometric data privacy, the Supreme Court began

34. WASH. REV. CODE § 19.375.010 (2017).

35. "Behavioral data" includes information relating to the "behavior" of a consumer, including, but not limited to: the products or content the consumer is interested in, the familiarity with brands, offers the consumer finds most attractive, and how much money the consumer is likely to spend on items. Lorna Keane, *How Behavioral Analytics is Transforming the Marketing Game,* GLOBALWEBINDEX (July 24, 2017), https://blog.globalwebindex.com/marketing/behavioral-analytics/.

36. CAL. CIV. CODE § 1798.140 (2018).

37. *Id.*

38. *Id.*

39. Note that California's Consumer Protection Act provides a "limited" private right of action, where consumers may only have a private right of action when their "nonencrypted and nonredacted personal information" is "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures." CAL. CIV. CODE § 1798.150(a) (2018). Furthermore, since the Illinois statute is the only current regulation to provide a private cause of action, and since California's statute was only just effectuated, the only current litigation surrounding biometric data privacy revolves around the Illinois statute. Without a private cause of action, citizens of other states have not had the opportunity to challenge the laws on the basis of their injuries due to the breaches of privacy.

discussing privacy in the technology industry beginning in 2001 with *Kyllo v. United States*.[40]

Kyllo v. United States acted as a spearhead for privacy when technology began advancing.[41] In *Kyllo*, the petitioner was inside his home when police used a thermal-imaging device to scan the complex and determine if there were heat amounts consistent with the heat produced by lamps used to grow marijuana.[42] After the scan showed that portions of the petitioner's complex were slightly hotter than the surrounding area, a warrant was issued to search the petitioner's home, and marijuana was found growing.[43] The Supreme Court ultimately held that the use of thermal-imaging to search the petitioner's residence was unlawful because the Government used a device that is "not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion;" the use of the technology constituted a "search" and therefore was unreasonable without a warrant.[44]

Although *Kyllo* did not discuss facial recognition technology, it is questionable whether facial recognition technology similarly constitutes a Government-used device "not in general public use" since the government's use of the technology differs greatly than the uses of individuals.[45] While facial recognition technology as a whole has become increasingly utilized by the public, the government's use of the technology appears to differ greatly from the public's use of the technology.[46] Therefore, it is possible that the application of regulations to the government may apply differently than the applications to private companies.

B. Companies' Regulation and Policies of Facial Recognition Technology

As companies continue to technologically advance and utilize facial recognition technology, it has become more important for companies to ensure the safety and privacy of these technologies in order to appease users. While some states have begun to regulate the use of the technology, companies and business owners have begun to set forth their own regulations and policies to ensure compliance with the varying regulations in place across the country.

---

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

41. *See generally id.*

42. *Id.* at 29.

43. *Id.* at 30.

44. *Id.* at 40.

45. *Id.* at 39 n.6 (acknowledging the dissent's argument that "general public use" may be a factor to consider in the constitutional analysis, but since thermal imaging is not "routine," its status as a factor would not be discussed in this case).

46. *Compare supra* notes 6–7 (discussing private uses of the technology to unlock phones and identify pictures), *with supra* notes 9–12 and accompanying text (discussing government use of the technology to survey crowds and identify individuals).

Apple tells users that any data collected from the Face ID technology, "including mathematical representations of your face," is encrypted and protected through the "Secure Enclave."[47] Apple describes the "Secure Enclave" as an extra layer of security that keeps the data secured, since the user never actually handles the data, thus making it difficult for the data to become compromised.[48] Although the Face ID data supposedly does not leave the device where the data is created, and is not backed up to a user's iCloud account, Apple provides an option for users to provide "Face ID diagnostic data," where data will be sent to AppleCare for support, thus transferring some of the information from the device.[49] Furthermore, although users may opt out from using the Face ID feature to unlock their phone, the iPhone automatically enrolls users in "Attention Aware Features," which still tracks a user's face to engage features of the phone, such as dimming the display if the user is not looking at the device.[50] Although users are able to deactivate this feature by actively turning it off in their Settings, it is still cause for concern that the Apple device default is to always watch its users.

Relatedly, Facebook's privacy policy states: "We don't share your template with anyone else but you."[51] Facebook also reassures users that the user's facial "template" will be saved while the user's account is active; however, the data is deleted if facial recognition is turned off.[52] Additionally, Facebook notes that facial recognition is only available to people who are over the age of eighteen.[53] Despite this seemingly helpful precaution, there is likely no way to safeguard against children claiming they are over the age of eighteen when they are in fact not.

The photo printing company Shutterfly also provides information regarding their use of users' data and facial biometrics. In their privacy policy updated January 1, 2020, Shutterfly states that as a user uploads photos, the user is automatically giving Shutterfly permission to access the photos stored on the user's device, along with any related "metadata."[54] If a user wishes to opt out of this, the user must "restrict the capture of image metadata" on the settings of their "image capture

47. *Supra* note 2.

48. *Storing Keys in the Secure Enclave*, APPLE, https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave (last visited Apr. 2, 2020).

49. *Supra* note 2.

50. *Id.*

51. *What is the face recognition setting on Facebook and how does it work?*, FACEBOOK, https://www.facebook.com/help/122175507864081 (last visited Apr. 2, 2020).

52. *Id.* ("If you turn your face recognition setting on, we'll keep your template while your account is active but will delete it if you turn your face recognition setting off.") Note that there is no mention of what will happen to the data once you delete your account. It seems as through the data will be deleted upon deletion of the account, but this is not explicitly stated as the deletion upon the facial recognition setting is so explicitly stated.

53. *Id.*

54. *Shutterfly, Inc. Online Privacy and Security*, SHUTTERFLY (Jan. 1, 2020) https://www.shutterflyinc.com/privacy.

device."[55] The privacy policy never defines "metadata," but notes that "metadata" is used to tag and organize photos uploaded.[56] Perhaps the most interesting section of the Shutterfly privacy policy is the section entitled "Supplemental Notice to California Residents."[57] This section explicitly states that only California residents have additional rights under the privacy policy, including the right to request information stored by Shutterfly and opt-out of "sales" of personal information to third parties.[58]

Although the regulations and policies of private companies appear to protect users' privacy, most companies default to an "opt-in" method, and users must proactively seek to "opt out" of their data usage. Each policy also seemingly includes language that appears to ensure users' data is "safe," but then speaks in overbroad terms and fails to define important words and phrases, such as "metadata." It is also concerning that privacy policies, such as that of Shutterfly's, now protects the privacy of California consumers differently than it protects the privacy of other consumers. The lack of consistency and clarity for users further illustrates the importance and need for federal regulations surrounding facial recognition technology.

II. THE BENEFITS OF FACIAL RECOGNITION TECHNOLOGY

Despite the lack of regulations, facial recognition technology has presented a plethora of benefits to society from traffic safety to medical advancements. Internationally, facial recognition technology has been used to prevent distracted driving.[59] In Australia, authorities have begun utilizing the technology of the Australian company Acusensus to help prevent distracted driving by installing camera systems above and on the side of roads to help detect "distracted drivers."[60] The cameras capture pictures of all cars passing by and search through the pictures to find drivers using their phones while driving.[61] If it is found that the driver is using a phone (and is thus deemed a "distracted driver"), the system will encrypt the image and send it to authorities.[62] However, if a distracted driver is not detected,

55. *Id.*

56. *Id.* ("We may analyze your photo content and metadata to help you tag and organize your photos and to make personalized product suggestions to you based on these photos…").

57. *See generally id.*

58. *Id.* The option for California residents to "opt-out" of sales of personal information is both interesting and confusing, most notably because earlier in the policy, Shutterfly states "We do not sell, license or share the personal information we collect with unaffiliated parties for their marketing purposes." *Id.*

59. Dinsan Francis, *AI-Powered Cameras Pitches to Fight Distracted Driving in Canada*, IPHONE IN CANADA (Aug. 26, 2019), https://www.iphoneincanada.ca/news/acusensus-catch-distracted-drivers/.

60. *Id.*

61. *Id.*

62. *Id.*

the system immediately deletes the picture.[63] Acusensus recently presented the technology at an international conference to countries including Canada, thus posing the possibility that this technology will continue to be utilized by more countries across the globe.[64]

Similarly, facial recognition technology has been utilized in America to help increase public safety. In August of 2019, police in New York used facial recognition technology to track down an accused rapist in less than twenty-four hours after the alleged attack.[65] The technology, Facial Identification Section, compared video footage from a nearby food store to mug shots that had previously been taken of the suspect.[66] New York Police Department officers noted that typically, a case such as this wouldn't be solved due to the "resources and manpower" it takes to identify a suspect.[67] Perpetrators in crimes of violence such as this one are typically repeat offenders—thus, facial recognition technology is able to quickly aid law enforcement's search and prevent future offenses.[68]

Facial recognition technology also provides numerous benefits to consumers. In an era where data is so easily accessible, it becomes increasingly important to protect this data. Facial recognition technology allows users to engage in "multifactor biometrics" to verify a user's identity, such as voice and facial recognition.[69] Companies such as Apple have begun using multifactor biometrics and facial recognition technology as a method to unlock phones.[70] Similarly, companies such as Google have developed technology that is able to recognize a user's voice, such that its Google Home responses may be tailored to the specific user, or may not respond at all to users who it does not recognize.[71]

Perhaps one of the most unlikely benefits of facial recognition technology is found in the medical field. According to a study from June 2014, scientists from

63. *Id.*

64. *Supra* note 59.

65. Craig McCarthy, *Facial Recognition Leads cops to Alleged Rapist in Under 24 Hours*, N.Y. POST (Aug. 5, 2019), https://nypost.com/2019/08/05/facial-recognition-leads-cops-to-alleged-rapist-in-under-24-hours/.

66. *Id.* The perpetrator had been previously arrested for raping a seventy-three-year old woman, but had been out on $10,000 bail. illustrating the usefulness of facial recognition technology's ability to prevent a repeat offender from continuing to commit crimes. *Id.*

67. *Id.*

68. *Id.* ("arrests in rape cases [are] notoriously low [] because of the resources and manpower it takes to identify a suspect, and the crime is historically repeated – and often escalated.").

69. Kevin DiGrazia, *Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach*, 13 J. BUS. & TECH. L. 255, 272 (2018) ("One of the most popular options proposed by security experts is to utilize multifactor biometrics to verify a person's information such as voice/facial recognition, iris scans, and fingerprints.") (*citing* Kaya Yurieff, *Why are we still using Social Security numbers as ID?*, CNN (Sept. 13, 2017, 8:40 AM), http://money.cnn.com/2017/09/13/technology/social-security-number-identification/index.html.)

70. *See supra* notes 47–49 and accompanying text.

71. Selena Larson, *Google Home now recognizes your individual voice*, CNN (Apr. 20, 2017), https://money.cnn.com/2017/04/20/technology/google-home-voice-recognition/index.html.

Oxford have reportedly developed a facial recognition program that is able to diagnose rare genetic conditions, such as Down Syndrome, through the observation of an ordinary photo.[72] For many rare disorders, there is no genetic test and thus may only be diagnosed through a specialist's analysis of facial features, as these rare genetic conditions are often accompanied by abnormal facial features.[73] However, these specialists are rare to find—therefore, with a developed facial recognition technology, more individuals with rare disorders will have access to a medical diagnosis.[74]

Most recently, facial recognition technology has been utilized in China to help combat the COVID-19 pandemic.[75] The Chinese government used the technology to track citizens' movements and prevent infected individuals from traveling.[76] The facial recognition technology allowed the government to identify individuals who were "more likely" to have contracted the virus, and similar technology was used to purportedly identify those who may have a fever.[77] This facial recognition technology was used in conjunction with a "monitoring system" that used big data to "identify and asses[] the risk of each individual" by examining travel history and potential exposure to those carrying the virus.[78] Although China was allegedly able to slow and eventually stop the spread of COVID-19 within the country, the use of the technology is unsurprisingly controversial, with some critics calling it "extreme"

72. Seema Mohapatra, *Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation*, 43 PEPP. L. REV. 1017, 1019–22 (2016) (noting that this is largely possible because rare genetic conditions are often accompanied by abnormal facial features) (citing Chris Weller, *Rare Genetic Disorders Could Be Diagnosed with Facial Recognition Computer Software,* MED. DAILY (June 24, 2014), http://www.medicaldaily.com/rare-genetic-disorders- could-be-diagnosed-facial-recognition-computer-software-289688 (stating that the software has not been used to formally diagnose as of yet, but is rather used to help assist physicians)).

73. *Id.* at 1022 (citing John Lynn, *A Biometrically Controlled Healthcare System,* EMR, EHR & HIPPA (Sept. 6, 2013), http://www.emrandhipaa.com/tag/facial-recognition/). Approximately thirty to forty percent of all rare genetic disorders impact facial formation and can thus be detectable with facial recognition technology. *Id.* (citing Brian Stallard, *Face Recognition Software Diagnoses Rare Disorders,* NATURE WORLD NEWS (June 24, 2014), http://www.natureworldnews.com/articles/7746/20140624/new-face- recognition-software-diagnoses-rare-disorders.htm.).

74. *Id.* at 1022.

75. *See generally* Khari Johnson, *How People are Using AI to Detect and Fight the Coronavirus*, VENTUREBEAT (Mar. 3, 2020), https://venturebeat.com/2020/03/03/how-people-are-using-ai-to-detect-and-fight-the-coronavirus/.

76. Khari Johnson, *AI Weekly: Coronavirus, Facial Recognition, and the Future of Privacy*, VENTUREBEAT (Mar. 6, 2020), https://venturebeat.com/2020/03/06/ai-weekly-coronavirus-facial-recognition-and-the-future-of-privacy/.

77. Bernard Marr, *Coronavirus: How Artificial Intelligence, Data Science and Technology Is Used To Fight The Pandemic*, FORBES (Mar. 13, 2020), https://www.forbes.com/sites/bernardmarr/2020/03/13/coronavirus-how-artificial-intelligence-data-science-and-technology-is-used-to-fight-the-pandemic/#5ccc29215f5f.

78. *Id.*

and "aggressive."[79] The use of facial recognition technology to combat COVID-19 with such controlling techniques illustrates the possibility for the technology to offer positive benefits along with very serious concerns.

III. THE CONCERNS WITH FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology has certainly developed over time but is still far from perfect. According to AI Now's 2018 Report, facial recognition technology raises concerns for racial and other biases—most notably, Amazon's Rekognition [sic] technology[80] falsely identified non-white individuals with an error rate of forty percent, whereas the technology only misidentified five percent of white individuals.[81] Furthermore, findings have shown that facial recognition technology is typically better at detecting light-skinned people than dark-skinned people, and better at detecting men than women.[82] This creates serious civil rights concerns and potentially furthers racial bias in the criminal justice system.[83]

Even when accurate, facial recognition technology creates many privacy and safety concerns. For example, although Australia's use of facial recognition technology to prevent "distracted driving" may assist in lowering the accidents resulting from such distracted driving, it raises questions of whether or not the pictures taken invade the privacy of all drivers.[84] Most notably, in America, this would become a question of whether or not the pictures taken violate the Fourth Amendment.[85]

---

79. Kai Kupherschmidt & Jon Cohen, *China's Aggressive Measures have Slowed the Coronavirus. They may not Work in other Countries*, SCIENCEMAG (Mar. 2, 2020), https://www.sciencemag.org/news/2020/03/china-s-aggressive-measures-have-slowed-coronavirus-they-may-not-work-other-countries (Lawrence Goston, a global health law scholar, noting, "I think there are very good reasons for countries to hesitate using these kinds of extreme measures.").

80. Amazon's Rekognition technology claims that it is able to "identify objects, people, text scenes, and activities in images and videos" and provide "highly accurate facial analysis and facial search capabilities…to detect, analyze and compare faces for a wide variety of user verification…and public safety use…" *Amazon Rekognition*, AMAZON, https://aws.amazon.com/rekognition/ (last visited Apr. 2, 2020).

81. Meredith Whittaker et al., AI Now Report 2018, AI NOW INSTITUTE, at 16 (Dec. 2018) (discussing a study conducted by the University of California Berkley, where it compared photos of members of Congress with the photos of 25,000 people who had been arrested. Amazon's Rekognition falsely identified 28 members of Congress as people from the database).

82. *Id.* (citing Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. OF MACHINE LEARNING RES. 77 (2018)).

83. *Id.* Amazon attributed the Rekognition errors to the fact that the facial recognition database is not "appropriately representative." *Id.* Furthermore, because of the racial biases in the American criminal justice system, most law enforcement databases that would use the technology would not be "appropriately representative," and thus continue to further the racial bias in the system by misidentifying individuals, and specifically non-white individuals. *Id.*

84. *Supra* note 59.

85. The Fourth Amendment states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…" U.S. CONST. amend. IV. It is

In addition to the civil rights concerns and racial bias in the criminal justice system, law enforcement's use of facial recognition technology has the potential to create serious concerns for general public safety and welfare. This is evident from the use of facial recognition technology in the Hong Kong Protests. In June of 2019, protests began in Hong Kong over a controversial extradition bill.[86] By August of 2019, the protests grew into a wider resistance movement, with Hong Kong police arresting nearly 750 people.[87] These arrests caused the people of Hong Kong to worry over how they were and currently are being tracked—the answer to these concerns being facial recognition technology.[88] Hong Kong had begun utilizing facial recognition technology at places such as border entrances, allowing the government to track and identify individuals through facial scans.[89] Citizens of Hong Kong eventually began using laser pointers during their protests to avoid the facial recognition cameras that Hong Kong police were using to track and arrest individuals.[90]

Despite Hong Kong's existing regulations designed to purportedly "protect" data privacy, the ordinance's vagueness and government exemptions seemingly do not protect citizen's data at all. [91] The government's misuse of facial recognition technology during the Hong Kong Protests exemplifies the concerns surrounding facial recognition technology and the government—without clear, distinct boundaries on the government's use of facial recognition technology, the technology may be used far beyond its intended purpose and beyond the scope of protection for citizens.

Another serious concern is the potential for data breaches in facial recognition technology. When an account or social security number is breached, the password or number can be changed and replaced.[92] However, when a fingerprint or facial recognition is compromised, there is no way to replace it—once a breach has

possible that searches into the cars of individuals through the pictures, without probable cause, would violate this amendment.

86. Rosalind Adams, *Hong Kong Protesters Are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched*, BUZZFEED NEWS (Aug. 17, 2019), https://www.buzzfeednews.com/article/rosalindaams/hong-kong-protests-paranoia-facial-recognition-lasers.

87. *Id.*

88. *Id.*

89. *Id.*

90. Alessandra Bocchi (@allesabocchi), TWITTER (Jul. 31, 2019, 6:35 AM), https://twitter.com/alessabocchi/status/1156513770254012416.

91. Personal Data (Privacy) Ordinance, No. 486, (1995) 81 O.H.K § 1. While there is "legislation" in place, it is very broad and full of exceptions, making it very difficult to enforce. These exceptions note that law enforcement may infringe upon the personal data rights when "safeguarding" security, defense, or international relations "in respect of Hong Kong." *Id.* at § 57. Without further specification, the exceptions make it almost impossible to actually protect citizens.

92. Kaya Yurieff, *Why are we Still Using Social Security Numbers as ID?*, CNN (Sept. 13, 2017, 8:40 AM) https://money.cnn.com/2017/09/13/technology/social-security-number-identification/index.html.

occurred, there is almost no way to remedy it.[93] As security experts note, "whatever the identifier is, it's still going to be the thing that attackers are going after."[94] Therefore, although the use of biometrics and facial recognition technology may be useful to protect data, unified system of facial recognition technology may not be the safest option until regulations are in place to control the systems by which the biometrics are collected.

IV. BALANCING THESE BENEFITS: THE NEED FOR REGULATION

Soon after September 11, 2001, the public began discussing the use of facial recognition technology to combat terrorism.[95] This was one of the first nationwide discussions regarding balancing the benefits of facial recognition technology for public safety, with the privacy concerns created by the use of the technology.[96] However, the perception of facial recognition has seemingly changed as the terrorism of 9/11 is no longer on the forefront of citizens' minds.

In order to balance the aforementioned benefits of facial recognition technology with the concerns, regulations must be implemented. These regulations should apply to both the government and to private companies that collect facial recognition data. There regulations should not outright ban the use of the technology—"[b]anning this technology for its negative potential is like banning the use of automobiles because there is a chance they could be involved in accidents."[97] Although there should not be an outright ban, implemented regulations may still prevent said concerns, similar to seatbelts preventing injuries. Regulations should be created with accountability, transparency, and privacy in mind.

A. Accountability

The first step to regulating facial recognition technology should be to ensure that all users of the technology are held accountable for their uses of the technology. Although federal statutes would ensure uniformity across the nation for the proper and improper uses of the technology, it is important that citizens are able to exercise their own rights to ensure the technology is being used properly. This

93. *See* 740 ILL. COMP. STAT. 14/5(c) (2008) ("Biometrics are unlike other unique identifiers…once compromised, the individual has no recourse, is at heightened risk for identify theft, and is likely to withdraw from biometric-facilitated transactions.").

94. *Supra* note 92.

95. *See* Susan McCoy, *O' Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUTER & INFO. L. 471, 482–83 (2002) ("safety and security of common everyday activities…is of the utmost importance to the general public considering the recent terrorists attacks directed at the innocent citizens of this country. Facial-recognition technology is an effective and efficient method of securing out country[]…").

96. *Id.*

97. *Id.* at 483.

would most efficiently be accomplished by providing citizens with a private right of action regarding the use of facial recognition technology.

In line with the Illinois statute,[98] violations of biometric privacy acts should provide a private right of action for citizens. Absent a private right of action, any violations of biometric privacy would be left in the hands of the government to decide whether or not to get involved, rather than up to the citizens whose privacy was violated. Including a provision with a private right of action for citizens would increase accountability for both law enforcement and private companies utilizing facial recognition technology.

The private right of action is historically important to the American judicial system and is something that European advocates have attempted to model.[99] American reformers originally pushed for a private right of action for citizens with a desire to create a more efficient legal system and make it easier for individuals with meritorious claims to "have their day in court."[100] The importance of a private right of action has been illustrated most notably through antitrust enforcement. Following the Sherman Act of 1890, courts began to recognize substantive rights of plaintiffs and encouraged private actions, which in turn increased the awareness of issues in antitrust.[101]

Similarly, a private right of action for the misuse of biometrics would increase awareness of the issues surrounding the technology. Although *Rosenbach v. Six Flags Entertainment Corporation* illuminated the potential weaknesses and flaws of the Illinois Biometric Information Privacy Act,[102] no other state statute allows a private cause of action making it impossible to challenge these statutes unless the government chooses to interfere.[103] A private cause of action would allow citizens to draw attention to the issues surrounding facial recognition technology and biometric privacy, and would help hold both private corporations and the government accountable for their uses of the technology.

B. Transparency

The second step to effectively regulating facial recognition technology is ensuring that companies and governments utilizing the technology are transparent and honest with users about the uses of the technology. Following the Illinois Biometric Information Privacy Act, federal facial recognition technology regulations should

98. 740 ILL. COMP. STAT. 14/20 (2008).

99. JOHN H. BEISNER & CHARLES E. BORDEN, *Expanding Private Causes of Action: Lessons from the U.S. Litigation Experience*, INSTITUTE FOR LEGAL REFORM, at 2 (Aug. 31, 2005) (ebook).

100. *Id.* at 2.

101. Arthur R. Miller, *Of Frankenstein Monsters and Shining Knights: Myth, Reality, and the "Class Action Problem,"* 92 HARV. L. REV. 664, 672–73 (1979).

102. *See supra* notes 16–18 and accompanying text.

103. *See* discussion *supra* Section I.A.

require all companies utilizing the technology to publicize their privacy policy.[104] As noted, most companies today that provide some type of "privacy policy" are often intentionally vague and exclude definitions and specifics as to the usage of the data collected.[105] To combat these issues and encourage transparency with users, the federal regulations should also specify exactly what information should be required in these privacy policies. For example, just as the Illinois statute requires private entities to develop a written policy and establish a "retention schedule" for the information collected,[106] the federal regulation should specify further what is required in a "retention schedule," allowing for proper usage of the technology, but ensuring that companies do not retain the information for longer than necessary.

The federal regulations should also provide a list of definitions for specific facial recognition technology words and phrases to ensure consistency across the country. Although the few state statutes in place now provide definitions for similar words, such as "biometric identifier," their definitions vary greatly and create serious inconsistencies. [107] In order to create transparency for citizens and provide a uniform understanding of the type of information that is protected from both private usage and government usage, the federal regulation should specify a definition for these words, and other words commonly used in the facial recognition technology field. The creation of consistent requirements and definitions for private corporations and governments utilizing facial recognition technology will ensure uniformity throughout the United States and ensure that all citizens are equally informed about their rights regarding the technology.

C. Privacy

Lastly, federal facial recognition technology regulations should ensure and protect the privacy of all citizens, as one of facial recognition technology's most concerning aspects is the potential violation of citizens' privacy by both law enforcement and private companies. Although facial recognition technology provides benefits in the criminal justice system,[108] federal regulations must support these benefits while ensuring the privacy of citizens and guaranteeing safety from "unreasonable

104. 740 ILL. COMP. STAT. 14/15 (2008).

105. *See supra* note 54 and accompanying text.

106. 740 ILL. COMP. STAT. 14/15 (2008).

107. *Compare* CAL. CIV. CODE § 1798.100 (2018) (defining biometric information as "an individual's physiological, biological, or behavioral characteristics, including an individual's…DNA…that can be used, singly or in combination with each other or with other identifying data to establish individual identity…"), *with* TEX. BUS. & COM. CODE § 503.001 (2009) (defining biometric information as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry").

108. *See supra* notes 65–68 and accompanying text.

searches and seizures" of the government.[109] This may be accomplished by allowing law enforcement's use of the technology, but with certain limitations.

In 1956, Maryland passed the Wiretapping and Electronic Surveillance statute.[110] This statute prohibits the private recording of conversations, exclusive of certain police activity, such as engaging in a criminal investigation with reasonable cause, or where an officer's safety may be in jeopardy.[111] However, under the statute, officers may not record private conversations absent these specified circumstances.[112] Following the structure of the Maryland Wiretapping and Electronic Surveillance statute, the use of facial recognition technology by law enforcement should also be prohibited under the federal regulations, exclusive of certain activity. In private places, such as homes and cars, the government and law enforcement should not be allowed to use facial recognition devices absent a warrant. However, due to the potential benefits of the technology, the devices may be used in public places if there is probable cause, similar to the Maryland Wiretapping and Electronic Surveillance statute.

A regulation structure such as this is also supported by *Kyllo*. While the Supreme Court held that thermal imaging devices should not be used to examine a private home since the devices were not "in general public use" and were used "to explore details of the home that would previously have been unknowable without physical intrusion,"[113] the usage of facial recognition technology to monitor drivers, such as Australia's usage of the technology,[114] similarly constitutes a physical intrusion. Therefore, any use of the technology to monitor drivers or individuals in their home, without their consent, should be explicitly prohibited by federal statute in order to ensure uniformity across the country.

Additionally, in order to ensure privacy and autonomy in private uses of the technology, citizens should have the right to choose whether to engage or not engage in the usage of facial recognition technology. Federal regulations should always allow an exception for citizen consent to engage in law enforcement or private corporations' use and retention of the information. However, as of now, most private companies' policies seem to indicate a default method of privacy that automatically opts users "in" to the data usage, and requires users to actively opt "out."[115] Federal regulations should instead require that the default method of privacy opts users "out" of the data collection and usage unless users actively consent to engage in the technology. By providing citizens with the autonomy to

109. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…").

110. MD. CODE ANN., CTS. & JUD. PROC. § 10-402.

111. *Id.*

112. *Id.*

113. Kyllo v. United States, 533 U.S. 27, 40 (2001).

114. *See supra* notes 59–64 and accompanying text.

115. *See supra* text accompanying note 50.

engage in facial recognition technology, and by closely regulating law enforcement's usage of the technology without citizen consent, all citizens, regardless of their location or jurisdiction, would have their privacy protected from unwarranted intrusions.

CONCLUSION

Although facial recognition technology provides a number of benefits to society, it is important to create legislation at the federal level to ensure uniformity across the nation, and ensure that all citizens enjoy their privacy, free from unwanted government or commercial intrusion. The state legislation in place as of now has taken a step in the right direction, but there is still an increasing need for legislation at a federal level, providing all citizens with the equal right to privacy. This can only be accomplished with federal regulations that specifically address the concerning areas of facial recognition technology and provide citizens with accountability, transparency, and privacy.