FACIAL RECOGNITION TECHNOLOGY: CAN WE TAME THE WILD WEST?

Angela M. Nieves*

TABLE OF CONTENTS

* Juris Doctor Candidate, St. Thomas University School of Law; ST. THOMAS LAW REVIEW, Managing Editor 2020; Bachelor of Arts in Liberal Studies, Florida International University, 2008.

I. INTRODUCTION: THE PROBLEM WITH FACIAL RECOGNITION TECHNOLOGY

A. Background

Facial recognition technology ("FRT") is a biometric resource that identifies individuals by analyzing physiological or behavioral characteristics and matching them to a database of named persons.[1] It has come a long way from its beginnings in research labs in the 1960s and 70s.[2] The use of cameras for surveillance and identification can be traced back several decades, when businesses and city authorities would install closed-circuit television (CCTV) cameras to film small areas of interest.[3] To make an identification later, officials would pore over tapes of recorded footage in search of helpful images and details and then compare these against the database of information in their possession, a process which was obviously time-consuming and labor-intensive.[4] Today, advances in science mean law enforcement agencies can have even real-time digital matches in just seconds, and the proliferation of cameras makes mass surveillance a possibility.[5]

---

[1] *See* Rosie Brinckerhoff, *Social Network or Social Nightmare: How California Courts Can Prevent Facebook's Frightening Foray into Facial Recognition Technology From Haunting Consumer Privacy Rights Forever*, 70 FED. COMM. L.J. 105, 112 (2018).

[2] *See* Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy.*, 23 B.U. J. SCI. & TECH. L. 88, 93 (2017); *see also* Shaun Raviv, *The Secret History of Facial Recognition*, WIRED (Jan. 21, 2020 6:00 AM), https://www.wired.com/story/secret-history-facial-recognition/ (describing the advancements made in early facial recognition technology).

[3] *See* Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, INTERCEPT (Jan. 27, 2020 12:53 PM), https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/ (discussing the early surveillance uses of cameras).

[4] *See* HERMAN KRUEGLE, CCTV SURVEILLANCE: VIDEO PRACTICES AND TECHNOLOGY 276 (Elsevier ed., 2011) (explaining that the operation of real-time video recording systems and later VHS recording systems was cumbersome and inefficient).

[5] *See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy Tech. & the Law. Comm. on the Judiciary*, 112th Cong. 19 (2012) [hereinafter *Privacy and Civil Liberties Hearing*] (statement of Larry Amerson, Sheriff, on behalf of the National Sheriff's Association) (detailing how results from facial

The technology is not limited to identification through surveillance, however. Social media networks and digital providers employ the technology on their websites and mobile applications to enhance consumer experience as well as engage new users.[6] Both the public and private sectors use FRT for a growing list of business and security uses.[7] For example, retail stores can identify repeat shoplifters,[8] transportation agencies can positively verify passengers prior to any boarding,[9] companies can have their employees clock in with a face scan,[10] and cars can alert drowsy or distracted drivers.[11] In countries like Russia and Sweden, everyday citizens can use mobile phone apps to identify strangers on the street.[12] It is an inarguable fact that the ever-evolving science of facial recognition is a powerful tool in the hands of its user. But how exactly this technology is used, and how this use affects individuals and society as a whole, are topics that are hotly debated by FRT providers, consumers, legislators, academics, and rights advocacy groups.[13]

Many questions surround the appropriateness, legality, and even morality of facial recognition technology's ever-expanding capabilities, and its ever-growing prevalence in our modern society.[14] The technology has advanced at an astonishing pace in recent years, leading to its unchecked use in ways

---

recognition can be obtained in seconds); *see also* Thomas Ricker, *The US, Like China, Has About One Surveillance Camera for Every Four People, Says Report*, VERGE (Dec. 9, 2019 10:45 AM), https://www.theverge.com/2019/12/9/21002515/surveillance-cameras-globally-us-china-amount-citizens (explaining that the U.S. is nearly on par with China in terms of number of surveillance cameras).

[6] CHRISTOPHER ANGLIM, ET AL. PRIVACY RIGHTS IN THE DIGITAL AGE 192 (Grey House Publishing ed., 2016).

[7] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-621, FACIAL RECOGNITION TECHNOLOGY REPORT 32 (2015) [hereinafter *GAO Report*] (noting that the use of biometrics in the business and security screening sectors was growing).

[8] Brinckerhoff, *supra* note 1, at 113.

[9] *Facial Recognition Technology: Part II: Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 8 (2019) [hereinafter *Transparency Hearings*] (statement of Austin Gould, Assistant Administrator, Requirements and Capabilities Analysis, Transportation Security Administration).

[10] Khari Johnson, *Congress Moves Toward Facial Recognition Regulation*, VENTUREBEAT (Jan. 15, 2020 11:27 AM), https://venturebeat.com/2020/01/15/congress-moves-toward-facial-recognition-regulation/.

[11] Mark Phelan, *2020 Subaru Models Will Greet You, Help You Keep Your Eyes on the Road*, DETROIT FREE PRESS (Aug. 3, 2019 7:44 PM), https://www.freep.com/story/money/cars/mark-phelan/2019/08/03/subaru-driverfocus-outback-forester-legacy/1903279001/.

[12] Brinckerhoff, *supra* note 1, at 113.

[13] *See generally Privacy and Civil Liberties Hearing, supra* note 5.

[14] *See* Seema Mohapatra, *Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation*, 43 PEPP. L. REV. 1017, 1024 (2016) (explaining that different privacy and ethical concerns are raised with the use of FRT in medical, commercial, and security applications).

that alarm everyone from legislators to watchdog groups to even developers of FRT themselves,[15] who observe that it is being used in ways that potentially violate fundamental rights.[16] Due process advocates contend that FRT allows the government to monitor our every move which violates our right to privacy.[17] FRT developers and consumers also collect and use millions of photos obtained from civilians without their knowledge or consent, constituting a separate violation of privacy.[18] Civil liberties groups contend that awareness that the government is watching us and using FRT to identify us chills associational and expressive freedoms.[19] Civil rights advocates meanwhile are drawing attention to the fact that FRT seems to disproportionately affect minorities and certain socioeconomic groups.[20]

In spite of these and other growing concerns over the years, the federal government has failed to enact laws that explicitly regulate the use of FRT.[21]

---

[15] *See* Peter Trepp, *How Face Recognition Evolved Using Artificial Intelligence*, FACEFIRST (Jan. 07, 2020), https://www.facefirst.com/blog/how-face-recognition-evolved-using-artificial-intelligence/ (noting the number of FRT milestones since 2010 to highlight the speed with which it has developed); *see also* Shirin Ghaffary, *How To Avoid a Dystopian Future of Facial Recognition in Law Enforcement*, VOX (Dec. 10, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation (noting legislators' push for limiting FRT use by law enforcement, and Microsoft's and IBM's calls for government regulation of the FRT industry); *see also* Mike Masnick, *Facial Recognition Company Says It Won't Sell to Law Enforcement, Knowing It'll Be Abused*, TECHDIRTY (June 29, 2018 1:30 PM), https://www.techdirt.com/articles/20180627/17283340123/facial-recognition-company-says-it-wont-sell-to-law-enforcement-knowing-itll-be-abused.shtml (describing FRT developer Kairos' refusal to sell the technology to law enforcement because they would likely abuse and misuse it).

[16] *See* Nakar & Greenbaum, *supra* note 2, at 93 ("Perhaps most disconcerting about all of this is that we often don't know when FRT is employed, either by the government or by private actors. Moreover, we don't know, and might never know how that data is processed, correlated and used to discern new and potentially damaging information about us. Living with all of these unknowns can create substantial and pervasive harms, including, intentional or unintentional censorship, control and inhibition of our actions, and the emotional harm of constant monitoring.").

[17] *See infra* Section II.B.ii.

[18] *Id.*

[19] Nakar & Greenbaum, *supra* note 3, at 115.

[20] *See Facial Recognition Technology: (Part I) Its Impact on Our Civil Rights and Liberties: Before the H. Comm. on Oversight & Reform*, 116th Cong. 21 (2019) [hereinafter *Impact Hearing*] (statement of Andrew G. Ferguson, Professor of Law, Univ. of the D.C., David A. Clarke School of Law); *see also* Olivia Solon, *Facial Recognition Database Used by FBI is Out of Control, House Committee Hears*, GUARDIAN (Mar. 27, 2017 6:00 AM), https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports ("Inaccurate matching disproportionately affects people of color").

[21] *See GAO Report, supra* note 7, at 28 ("[W]e did not identify any federal laws that expressly regulate commercial uses of facial recognition technology in particular."); *see also*

Thus, the proper gathering, storage, and use of biometric records–such as photos of faces–have been left to the states to determine.[22] Where states have not acted, developers and users of FRT find themselves free to manage the process, and reports on secret deals and questionable activities have led to increasing apprehension about their stewardship of the biometric data collected.[23] FRT developers are even racing to adapt their systems to facial coverings that have become ubiquitous in the COVID-19 pandemic, without any real consensus or requirements from consumers or regulators.[24]

With almost no U.S. laws governing police or private use of FRT, and no systems to ensure accuracy and bias-free results, some are calling this the wild west of biometrics.[25] This article examines the ways FRT is used in the United States and its impact, current and potential, on our society. Part II sets out the differing claims about its value and its drawbacks, as seen through the eyes of the major stakeholders: private service providers, consumers such as police departments and retail businesses, and rights advocates. Part III discusses past legal responses to address those claims, and the factors that helped shape those responses. The analysis in Part IV attempts to draw from

---

Brinckerhoff, *supra* note 1, at 107 (explaining that in the US there is no one comprehensive federal law regulating privacy and the gathering, use, and storage of personal information).

[22] *GAO Report, supra* note 7, at 32.

[23] *See Impact Hearing*, *supra* note 21, at 6- 7 (statement of Neema Singh Guliani, Senior Legis. Counsel, ACLU) (stating that the FBI and other agencies have been expanding the use of FRT, and mostly secretly); *see also* NANCY YUE LIU, BIO-PRIVACY: PRIVACY REGULATIONS AND THE CHALLENGE OF BIOMETRICS, 73 (Routledge ed., 2012) (discussing the public's distrust of companies and government agencies handling their facial image data).

[24] *See* Mara Hvistendahl and Sam Biddle, *Homeland Security Worries Covid-19 Masks Are Breaking Facial Recognition, Leaked Document Shows*, THE INTERCEPT (July 16, 2020 2:10 PM), https://theintercept.com/2020/07/16/face-masks-facial-recognition-dhs-blueleaks (noting that FRT developers are "scrambl[ing] to adapt their systems to facial coverings"); *see also* Wudan Yan, *Face-Mask Recognition Has Arrived—For Better or Worse*, NAT'L GEOGRAPHIC (Sept. 11, 2020), https://www.nationalgeographic.com/science/2020/09/face-mask-recognition-has-arrived-for-coronavirus-better-or-worse-cvd (noting concern among experts about the lack of rules and federal guidelines with regard to data collection and use); *see also* Susan Miller, *Facial Recognition Adapts to a Mask-Wearing Public*, GCN (June 3, 2020), https://gcn.com/articles/2020/06/03/facial-recognition-masks.aspx (citing FRT developer NEC's advice to customers like the U.S. Customs and Border Patrol to "make their own decisions about the [updated] technology for now").

[25] *See* Ephrat Livni, *Facial-Recognition Technology Will Make Life a Perpetual Police Lineup For All*, QUARTZ (Mar. 26, 2017), https://qz.com/940979/facial-recognition-technology-will-make-life-a-perpetual-police-lineup-for-all (quoting Clare Garvie's comparison of the regulation and standard-free panorama to "a wild west"); *see also* DJ Pangburn, *Due To Weak Oversight, We Don't Really Know How Tech Companies Are Using Facial Recognition Data*, FAST COMPANY (July 5, 2019), https://www.fastcompany.com/90372734/due-to-weak-oversight-we-dont-really-know-how-tech-companies-are-using-facial-recognition-data ("It's every company for itself, it's the Wild West—there are no rules, there aren't any industry best practices").

current FRT trends a prediction of its practical and legal future in the U.S. Part V will evaluate the effectiveness of past responses and possible alternatives. In addition, it will propose solutions for this important struggle to balance the usefulness of FRT with individual rights, a difficult dilemma that America needs to solve sooner rather than later.[26]

B. A Leap in Biometric Data

Understanding the debates surrounding the use of FRT and its implications on individual rights requires at minimum a high-level explanation of biometrics and what facial recognition is. A person's biometric data are generally biological or behavioral features that are unique and verifiable, like fingerprints or voiceprints, which are used for identification purposes.[27] In FRT, the biometric is our facial image, which the technology uses to generate a digital file, or faceprint, after it has mapped out unique features that can be compared against other faceprints.[28] FRT analyzes and measures a person's features or behavioral characteristics in four steps.[29] It first detects a face in an image, and then analyzing the person's physical characteristics, uses an algorithm to create the faceprint.[30] Another algorithm then either verifies identity by accepting or denying the identity claimed, or it identifies the person by matching them to a database of known people.[31] The success of the technology is dependent upon the size of the database it has to draw upon; FRT thus requires an extensive number of faceprints for accurate results.[32]

---

[26] *See* AMOS N. GUIORA, CYBERSECURITY: GEOPOLITICS, L. & POL'Y, 77 (Routledge ed., 2017) (explaining that democratic societies like the U.S. must balance things like national security and the rights of individuals if they are to retain their character and purpose).

[27] Jeffrey Rosenthal & David Oberly, *Biometric Privacy In 2020: The Current Legal Landscape*, LAW360 (Feb. 3, 2020, 5:59 PM), https://www.law360.com/articles/1239794/biometric-privacy-in-2020-the-current legal-landscape [hereinafter Rosenthal & Oberly, *Legal Landscape*].

[28] Kimberly L. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 427 (2014).

[29] ANGLIM, *supra* note 6, at 190.

[30] *GAO Report, supra* note 8, at 3.

[31] ANGLIM, *supra* note 6, at 190.

[32] *See* Adrienne Lafrance, *The Ultimate Facial-Recognition Algorithm*, ATLANTIC (June 28, 2016), https://www.theatlantic.com/technology/archive/2016/06/machine-face/488969 (explaining that large datasets are needed to properly test the accuracy of FRT).

II. CONFLICTING CLAIMS AND PERSPECTIVES

A. Facial Recognition Technology Supporters

1. Creators and Vendors

The current technology has been created and developed by tech giants such as Amazon and Google, as well as lesser known companies who have worked hard to make it as ubiquitous as global positioning system (GPS) tracking.[33] Nowadays, facial recognition is commonly used to log in to a computer, authenticate a credit card transaction, or identify loved ones in photo management software.[34] FRT innovators minimize privacy concerns, preferring instead to tout the growing list of benefits that go beyond the convenience or "cool" factors.[35] For example, FRT is used to search through criminal mug shots to generate potential suspects, saving law enforcement agencies precious time and manpower.[36] FRT has also been used to locate missing persons as well as to identify unknown individuals.[37] In recent years, scientists have been able to use FRT to help diagnose around ninety rare genetic conditions using ordinary family photos.[38] FRT companies continue to push for more uses and better results, generally expressing a more nuanced view on the privacy rights of the people whose photos they use in the name of those technological advancements.[39]

FRT developers are also quick to point out that Americans have demonstrated a willingness to share private details about themselves,

---

[33] *See GAO Report, supra* note 7, at 6 (acknowledging that FRT is widely used commercially but the full extent of FRT is unknown); *see also* Trepp, *supra* note 15 (describing FRT as a feature as common in consumer products like GPS).

[34] *See* Rosenthal & Oberly, *Legal Landscape*, *supra* note 27 (describing common uses of biometric data).

[35] *See* Brad Smith, *Facial Recognition: It's Time for Action*, MICROSOFT ON THE ISSUES (Dec. 6, 2018), https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/ (stating that FRT has created "many new and positive benefits for people around the world.").

[36] See *Transparency Hearings*, *supra* note 9, at 3 (statement of Kimberly J. Del Greco, Deputy Assistant Director, Crim. Justice Information Services, Federal Bureau of Investigation) (explaining the general process of the FBI's FRT in assisting investigations).

[37] *See* Smith, *supra* note 35 (describing how FRT identified thousands of missing children in India in just four days, and how historians used FRT to identify previously unknown Civil War soldiers).

[38] Mohapatra, *supra* note 14, at 1022.

[39] *See* ANGLIM, *supra* note 6, at 190 (explaining how FRT is become more accurate every day); *see also Transparency Hearings*, *supra* note 9, at 4 (statement of Kimberly J. Del Greco) (describing the improved accuracy rate of the FBI's facial recognition program).

including their images, on a growing number of online sites.[40] Consumers almost immediately embraced facial recognition as a convenient means for accessing smartphones and tagging pictures, and as other industries incorporate FRT into their products, consumer demand for the technology has risen.[41] In response, tech giants Amazon, Apple, Facebook, Google, and Microsoft have each filed facial recognition patent applications.[42] Additionally, developers argue that Americans do not see FRT as exceedingly invading their privacy for two principal reasons. First, the data is collected in public, where people tend to expect less privacy and anonymity.[43] Second, most people feel collecting a photo of a person is not as intrusive as other biometrics such as fingerprints.[44] Thus, FRT providers argue most people are willing to endure some loss of privacy in exchange for the technology's benefits, which include convenience, security, but also the tremendous economic growth it has brought about.[45] Thanks to its multi-purpose nature, analysts predict the facial recognition market will reach over $12 billion by 2025.[46]

2. Consumers of Facial Recognition Technology

Businesses in the private sector have steadily become supporters of FRT, finding commercial potential in innovative, industry-specific applications of the technology.[47] Retail stores and shopping malls, for instance, employ the

---

[40] *See* ANGLIM, *supra* note 6, at 190 (Grey House Publishing ed., 2016) (describing how individuals create a FRT repository by uploading billions of photographs to the internet).

[41] *See* Nakar & Greenbaum, *supra* note 2, at 93 (explaining that facial recognition systems will become more pervasive thanks to strong consumer demand).

[42] Natasha Singer, *Facebook's Push for Facial Recognition Prompts Privacy Alarms*, N.Y. TIMES (July 9, 2018), https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html.

[43] YUE LIU, *supra* note 23, at 171.

[44] *Id.* at 30.

[45] *See* GUIORA, *supra* note 26, at 28 (discussing a willingness to tolerate impositions on privacy in the name of protection); *see also* ANGLIM, *supra* note 6, at 191 (asserting various trade-offs that FRT provides).

[46] *See* Nakar & Greenbaum, *supra* note 2, at 96 ("FRT is already implemented in many areas such as security, commerce, social media, personal use, and even for religious purposes."); *Facial Recognition Market to Hit $12 Billion by 2025 - Global Insights on Top Trends, Key Technologies, Competitive Landscape, New Investments, Strategic Initiatives, and Business Opportunities: Adroit Market Research*, GLOBENEWSWIRE (last visited Apr. 21, 2020), https://www.globenewswire.com/news-release/2020/01/27/1975200/0/en/Facial-Recognition-Market-to-hit-12-billion-by-2025-Global-Insights-on-Top-Trends-Key-Technologies-Competitive-Landscape-New-Investments-Strategic-Initiatives-and-Business-Opportun.html [hereinafter *Facial Recognition Market to Hit $12 Billion*].

[47] *See* Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores*, INTELLIGENCER (Oct. 20, 2018), https://nymag.com/intelligencer/2018/10/retailers-

technology, using security cameras as well as cameras in digital signs and kiosks, to track shoppers' habits and gauge their attention to ads.[48] Retailers and advertisers can then adjust advertisements accordingly in real time, which can potentially lead to more sales.[49] Restaurants are using FRT to enhance customers' ordering experience, allowing them to use self-service kiosks to quickly and easily reorder their favorite meals.[50] Simplifying this process often means more orders for the restaurant and the ability to shift labor to other areas of need.[51]

A growing number of business establishments are also using FRT to enhance service for repeat customers or deny service to *personae non gratae*.[52] Hotels are beginning to use facial recognition to welcome returning guests with personalized greetings and speedy check ins.[53] Cruise lines use FRT to facilitate faster embarkation and debarkation of passengers, as well as to help them access photos of themselves taken throughout their cruise.[54] In the hospitality industry, these kinds of measures, which provide for a more personalized and frictionless customer experience, are key to attracting and retaining loyal customers,[55] a principal source of revenue. The private sector additionally uses FRT for risk management: stores large and small use it to

---

are-using-facial-recognition-technology-too.html (describing various uses of FRT in retail stores).

[48] Tabor, *supra* 47; *see also* Debra Cassens Weiss, *Macy's Uses Facial Recognition Software to Identify Customers on Security Cameras, Lawsuit Claims*, ABA JOURNAL (Aug. 12, 2020 3:36 PM), https://www.abajournal.com/news/article/suit-claims-macys-uses-facial-recognition-software-to-identify-customers-on-security-cameras (detailing a lawsuit filed in Illinois against Macy's alleging the retailer used FRT to identify unknowing customers for improved marketing and security).

[49] *GAO Report, supra* note 7, at 9.

[50] *When Restaurant Tech Sees Your Face and Identifies Your Taste*, PYMNTS (Nov. 5, 2019), https://www.pymnts.com/restaurant-innovation/2019/malibu-poke-facial-recognition-technology-self-service-kiosks/.

[51] *Id.*

[52] *See* Brinckerhoff, *supra* note 1, at 114 (describing how FRT can be used to identify repeat customers as well as previous shoplifters).

[53] *E.g.*, Frank Wolfe, *Facial-Recognition Tech Creates Service, Security Options*, HOTEL MANAGEMENT (Oct. 10, 2019 11:11AM), https://www.hotelmanagement.net/tech/facial-recognition-tech-creates-service-security-options; *Facial Recognition in Retail & Hospitality*: Cases, Benefits, Laws, INTELLECTSOFT (Apr. 17, 2019) https://www.intellectsoft.net/blog/facial-recognition-in-retail-and-hospitality/.

[54] *Facial Recognition Technology*, CARNIVAL.COM, https://help.carnival.com/app/answers/detail/a_id/6019/~/facial-recognition-technology (last visited Apr. 21, 2020).

[55] *See 3 Ways Facial Recognition Tech Can Generate Revenue for Hotels*, HOSPITALITY TECHNOLOGY (Aug. 8, 2018), https://hospitalitytech.com/3-ways-facial-recognition-tech-can-generate-revenue-hotels (discussing three advantages to using FRT in the hospitality industry: creating enhanced customer experiences, augmenting a hotel's customer database, and increased security).

alert to previously identified shoplifters, and casinos use it to keep card counters out.[56] Moreover, the technology has been used in locations such as amusement parks and stadiums to ensure the safety of attendees; FRT has helped reunite lost children with their parents,[57] scan selfie-kiosks at concerts for known stalkers,[58] and detect persons banned from being on public school grounds.[59] With FRT developers providing the private sector with products that both generate revenue and limit risk, the technology is likely to continue enjoying support from those private organizations.[60]

Security being a top priority across all industries, FRT creators have marketed the technology to consumers in the public sector as well.[61] Law enforcement authorities have joined the growing group of agencies who purport to use FRT as an investigative tool.[62] The technology can be used when fingerprint identification fails, or when a suspect is uncooperative in identifying himself.[63] Recent studies have even demonstrated FRT algorithms are better than humans at identifying individuals from images captured under different lighting conditions.[64] Recognizing how FRT can enhance crime-solving and counter-terrorism capabilities, federal agencies like the Federal Bureau of Investigation ("FBI") have collaborated with over two dozen states to share databases and increase the likelihood of identification.[65] FRT supporters point to success stories, such as the positive

---

[56] Nakar & Greenbaum, *supra* note 2, at 99.

[57] *See* Singer, *supra* note 42 (relating Amazon's claim that its FRT is used at parks to find lost children).

[58] *See* Lane Brown, *There Will Be No Turning Back on Facial Recognition*, INTELLIGENCER (Nov. 12, 2019), https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html (explaining how FRT was used at several Taylor Swift concerts to check for known stalkers of the artist).

[59] Tom Simonite & Gregory Barber, *The Delicate Ethics of Using Facial Recognition in Schools*, WIRED (Oct. 17, 2019 6:00 AM), https://www.wired.com/story/delicate-ethics-facial-recognition-schools/.

[60] *See GAO Report, supra* note 7, at 7–10 (citing several different commercial uses for FRT).

[61] *See* Singer, *supra* note 42 (citing Amazon's marketing of its FRT to police departments); *see also GAO Report, supra* note 7, at 8–9 (listing the different commercial and security uses of FRT in the private sector).

[62] *See Transparency Hearings*, *supra* note 9, at 4 (statement of Kimberly J. Del Greco).

[63] *Id.* at 3 (statement of Kimberly J. Del Greco); *see also* Cade Metz & Natasha Singer, *Newspaper Shooting Shows Widening Use of Facial Recognition by Authorities*, N.Y. TIMES (June 29, 2018), https://www.nytimes.com/2018/06/29/business/newspaper-shooting-facial-recognition.html (describing the use of FRT to identify the suspect in the Capital Gazette killings).

[64] *See* RACHEL B. JEFFERSON, BIOMETRICS, PRIVACY, PROGRESS, AND GOVERNMENT, 31 (Nova Science Publishers ed., 2010).

[65] *See Privacy and Civil Liberties Hearing, supra* note 6, at 19 (statement of Larry Amerson) (extolling the ways FRT helps authorities fight terrorism and protect society at large); *see also* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America*, GEORGETOWN L. CTR. ON PRIVACY & TECH. (Oct. 18,

identification of imposters attempting to enter the U.S.,[66] and the capture of a pedophile who had eluded law enforcement for 20 years.[67] Government agencies such as the Transportation Security Administration ("TSA") and the U.S. Customs and Border Protection ("CBP") are using FRT at checkpoints across the nation, which they claim increases security effectiveness and enhances travelers' experience.[68] But the most common use of FRT by law enforcement is also the most controversial one: surveillance.

Given its origins in defense and law enforcement, it is unsurprising that surveillance is where facial recognition would truly surpass all other technologies.[69] The United States has approximately seventy million surveillance cameras installed, which is roughly one camera per four people, rivalling China's per person camera penetration rate.[70] Taken together with the fact that law enforcement facial recognition networks contain the images of over 117 million American adults and that the technology is continually improving in accuracy, authorities wield a powerful weapon that can be used to identify anyone practically anywhere, as well as monitor their every movement.[71] Agencies that use FRT for surveillance claim the goal is to ensure the security of the public, which is accomplished by running captured images against their databases in search for persons on a "hot list."[72] However, there are no laws establishing guidelines on the process, much less limits on its use.[73]

In 2015, police in Baltimore used FRT in conjunction with a social media platform to identify participants at a protest over the police shooting of

---

2016), https://www.perpetuallineup.org/ (explaining that FBI and law enforcement face recognition systems are increasingly accessing state driver license and ID photo databases).

[66] *See* TRANSPORTATION SECURITY ADMINISTRATION AND U.S. CUSTOMS AND BORDER PROTECTION: DEPLOYMENT OF BIOMETRIC TECHNOLOGIES REPORT TO CONGRESS, U.S. DEPT. OF HOMELAND SECURITY 17 (Aug. 30, 2019) [hereinafter TSA BIOMETRIC REPORT] (noting that as of April 2019, CBP had identified 130 imposters attempting to cross U.S. borders); *see also* Tajha Chappellet-Lanier, *CBP's Airport Facial Recognition Technology Catches Its First 'Imposter'*, FEDSCOOP (Aug. 24, 2018), https://www.fedscoop.com/cbp-facial-recognition-success/ (detailing the capture of a Congolese man attempting to use a French passport to clear an airport checkpoint).

[67] *See Transparency Hearings*, *supra* note 10, at 12 (testimony of Kimberly J. Del Greco).

[68] *Id.* at 12 (2019) (statement of Austin Gould).

[69] *See* Trepp, *supra* note 16 (explaining that FRT's roots are "firmly planted in the defense and law enforcement sectors.").

[70] *See* Ricker, *supra* note 6.

[71] *See* Garvie, Bedoya, & Frankle, *supra* note 66 (noting that over 117 million American adults are in law enforcement face recognition networks); *see also* L. Brown, *supra* note 59 (citing NIST test results in 2018 that were twenty times better than those in 2014).

[72] Garvie, Bedoya, & Frankle, *supra* note 66.

[73] *See Impact Hearing*, *supra* note 21, at 11 (statement of Cedric Alexander, former President, National Organization of Black Law Enforcement Executives).

Freddie Gray.[74] Officers were able to discover protesters with outstanding warrants and arrest them on the spot, during the exercise of their First Amendment right to assemble.[75] And while many would assume the police would infringe on fundamental rights only in the name of capturing the most dangerous of criminals, some police departments have taken to using facial recognition to apprehend even non-violent suspects.[76] With private business and home camera owners increasingly willing to plug their units into police networks to help the fight against crime, law enforcement agencies could soon have a vast network of cameras at their disposal, giving them complete surveillance of public spaces, [77] and without any laws, regulations, or checks systems.[78]

B. Rights Advocates

1. Consent is Key

In an era where consent is generally required, oftentimes even for the most banal of activities, opponents of FRT note that this technology has proliferated without express or sometimes even implied consent from the individuals whose photos developers use.[79] The vast majority of Americans are unaware that their photos have been taken, stored, used, and even sold by developers as the technology continues to evolve.[80] The data can also be

---

[74] *Id.* at 54 (statement by Rep. Elijah Cummings, Chairman of the Committee).
[75] *Id.*
[76] *See* Nakar & Greenbaum, *supra* note 3, at 97 (describing use of FRT to apprehend non-violent offenders).
[77] *See* Kwet, *supra* note 4 (describing the pervasiveness of cameras in public spaces).
[78] *See Impact Hearing*, *supra* note 21, at 11 (statement of Cedric Alexander).
[79] *See* Nakar & Greenbaum, *supra* note 3, at 96 (addressing concerns over consent and FRT).
[80] *See* Lauren Berg, *AI Biz Kept 'Face Database' Of OKCupid Profile Pics, Suit Says*, LAW360 (Feb. 14, 2020, 8:59 PM), https://www.law360.com/cybersecurity-privacy/articles/1244342/ai-biz-kept-face-database-of-okcupid-profile-pics-suit-says?nl_pk=9a283bed-c005-42eb-aa84-e064c4b54145&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy ("Clarifai Inc., an artificial intelligence company . . . secretly harvested the profile pictures of tens of thousands of users on the dating site OKCupid . . ."); *see also* Delia Paunescu, *The Government Keeps Its Use of Facial Recognition Tech Secret. The ACLU is Suing.*, VOX (Nov. 7, 2019 5:00 PM) https://www.vox.com/recode/2019/11/7/20953655/facial-recognition-technology-government-fbi-aclu-lawsuit-reset-podcast ("[B]ig tech companies like Amazon and Microsoft have been selling facial recognition tech to various companies for business purposes while Amazon is also selling its facial recognition capabilities directly to law enforcement agencies, despite the fact that most citizens have never consented to their faces being used for these purposes."); *see also* Solon, *supra* note 21 ("Approximately half of adult Americans' photographs are stored in facial recognition databases that can be accessed by the FBI, without their knowledge or consent . . .").

accessed by any government agency for any reason.[81] No doubt most people would be shocked to learn that the FBI has three facial recognition programs and access to over 640 million photos: only 36 million are criminal mug shots, the rest are civil in nature, passport and driver license photos of everyday law-abiding citizens.[82] Because the makers of FRT and their customers are not required to obtain consent from anyone or report any details on how the technology is being used, Americans are purposely kept in the dark as to when and how FRT is employed, and what happens to their data over time.[83] Furthermore, this lack of transparency allows FRT users to cover up data breaches and escape higher accountability for the mishandling of data, despite public scrutiny.[84] If facial recognition is here to stay, critics argue, the public must be notified when and how their data is being used, stored, and shared, and affirmative consent must be obtained beforehand.[85]

2. Due Process: Privacy Rights in Play

The right to privacy has been recognized as a fundamental human right

---

[81] *See* Josiah Wolfson, *The Expanding Scope of Human Rights in a Technological World--Using the Inter-American Court of Human Rights to Establish a Minimum Data Protection Standard across Latin America*, 48 U. MIAMI INTER-AM. L. REV. 188, 193 (2017) (explaining that an individual's private data may be: "(1) sold to private companies; (2) processed anywhere in the world; (3) accessed by a government agency without just cause; (4) stored for an indefinite period of time; and (5) used for an unintended purpose.").

[82] *See Transparency Hearings*, *supra* note 10, at 35, 47 (testimony of Dr. Gretta L. Goodwin, Director, Justice and Law Enforcement Issues, Homeland Security and Justice Team, U.S. Government Accountability Office).

[83] *See* Nakar & Greenbaum, *supra* note 3, at 93 (stating "we often don't know when FRT is employed, either by the government or by private actors"); *see also* Celeste Bott, *Surveillance Co. Clearview AI Hit With Biometric Privacy Suit,* LAW360 (Feb. 6, 2020 3:56 PM), https://www.law360.com/articles/1241502/surveillance-co-clearview-ai-hit-with-biometric-privacy-suit (describing a FRT company's covert harvesting of Illinois residents' photos and biometric data for profit).

[84] *See* John Fingas, *FTC Fines TikTok $5.7 Million Over Child Privacy Violations*, ENGADGET (Feb. 27, 2019), https://www.engadget.com/2019/02/27/ftc-fines-tiktok-over-child-privacy/ (citing social media company TikTok's $5.7 million penalty for collecting data from minors without appropriate consent, and making the profiles public despite "thousands of complaints"); *see also* Craig Giles & Zahra Deera, *TikTok Investigation Should Prompt More Data Transparency*, LAW360 (Feb. 21, 2020 4:27 PM), https://www.law360.com/cybersecurity-privacy/articles/1245489/tiktok-investigation-should-prompt-more-data-transparency?nl_pk=9a283bed-c005-42eb-aa84-e064c4b54145&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy (describing criticism of social media companies' secrecy of or failure in the handling of user data).

[85] *See Impact Hearing*, *supra* note 21, at 22, 30 (testimony of Joy Buolamwini, Founder, Algorithmic Justice League).

worldwide, and in the U.S. it is a protected right under the Fourth Amendment to the Constitution.[86] The illegal sharing of a person's sensitive information constitutes an invasion of privacy, a violation that becomes prevalent in times of war and terrorism, or under certain types of government.[87] During World War II for example, Nazi Germany partnered with International Business Machines (IBM) to create a system for collecting and synthesizing the data of the Jewish population in order to facilitate the Nazi master plan.[88] Today, civil liberties groups draw parallels to the collaborations between corporations like Amazon and government entities like police departments and Immigration and Customs Enforcement ("ICE").[89] It was recently revealed, for example, that unbeknownst to state residents, ICE uses FRT to check millions of driver license photos to find and deport undocumented immigrants, despite many of them having legally obtained those licenses in states like Washington, Utah, and Vermont.[90] In New York City, meanwhile, close to 3,000 arrests have been made using FRT, but most of the accused were not informed that FRT was used to identify them.[91] These and other examples of the intrusive nature of facial recognition and the serious consequences it can yield cause activists and academics alike to warn organizations that if they continue to ignore ethical concerns in their dealings, they run the risk of repeating the sins of IBM in the Nazi era.[92]

Rights activists also point out another disturbing trend that impinges on our right to privacy: beyond recorded and real-time surveillance, FRT is capable of identifying patterns, which pieced together become new

---

[86] 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, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); *see also* G.A. Res. 217A (III), Art. 12, U.N. Doc. A/810 (1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence . . . .").

[87] Alvar Freude and Trixy Freude, *Echoes of History: Understanding German Data Protection*, BERTELSMANN FOUNDATION (Oct. 1, 2016), https://www.bfna.org/politics-society/echoes-of-history-4tdtdjes5l/ .

[88] Wolfson, *supra* note 82, at 190.

[89] Anthony Cuthbertson, *Amazon Workers' 'Refuse' To Build Tech For US Immigration, Warning Jeff Bezos of IBM's Nazi Legacy,* INDEPENDENT (June 22, 2018), https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-workers-immigration-jeff-bezos-ibm-nazi-protest-a8411601.html.

[90] Bill Chappell, *ICE Uses Facial Recognition to Sift State Driver's License Records, Researchers Say*, NPR (July 8, 2019 4:23 PM), https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa.

[91] *Impact Hearing*, *supra* note 21, at 34 (testimony of Clare Garvie, Senior Associate, Center on Privacy & Technology, Georgetown University Law Center).

[92] Cuthbertson, *supra* note 90.

information that can be used to predict a person's movements.[93] By stringing together data collected over time from different cameras at different locations, FRT can predict where you will go next and what you will do, a kind of predictive analytics that can be used –and abused– by private businesses and law enforcement alike.[94] Rights advocates warn that the government in particular has access to multiple points of data (i.e. surveillance footage, phone call and email records, financial transactions, crime statistics) that make this kind of predictive analytics possible.[95] However, the Supreme Court in *Carpenter v. United States* recently held that using cell phone records to determine a suspect's locations over an extended timeframe amounted to a warrantless search under the Fourth Amendment and thus violated his right to privacy because such data could potentially reveal intimate details of his life that go beyond being spotted in public thoroughfares.[96] Thus, were FRT to be used to secretly gather data on a person's movements over an extended period of time, the Court could find that it too constitutes a violation of privacy rights.[97]

3. First Amendment Rights at Risk

Under the First Amendment to the Constitution, Americans have a right to freely express themselves and assemble peacefully.[98] Decades of jurisprudence have led to our conviction that government actions that tend to have a chilling effect on the open exchange of ideas or the free association of persons are an unconstitutional burden on our First Amendment rights.[99]

---

[93] *See* K. Brown, *supra* note 29, at 466 (explaining that FRT "identif[ies] patterns within such data which reveal new information that does not exist anywhere in isolation").

[94] *See* Nakar & Greenbaum, *supra* note 3, at 93 (citing the fact that although we know FRT can be used to glean new information, FRT users do not disclose "how that data is processed, correlated and used to discern new and potentially damaging information about us"); *see also* Smith, *supra* note 36 (explaining how biometric data could potentially be exploited by business).

[95] K. Brown, *supra* note 29, at 426–27.

[96] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (finding that the data on the suspect's locations over a four-month period constituted a warrantless search that violated his Fourth Amendment right to privacy).

[97] *See* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, A.B.A. (last visited Apr. 21, 2020) https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/.

[98] U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . or the right of the people peaceably to assemble . . . ").

[99] *See* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166–67 (2002) (holding that a permit requirement for door-to-door solicitation placed an undue burden on the freedom of expression because it would inhibit some speech by persons wishing to remain anonymous, as well as outright ban spontaneous speech); *see also* Lamont

Courts have additionally upheld an individual's right to anonymous speech and association.[100] Opponents of FRT point out that the technology is often sold –secretly– to government agencies without the proper training or understanding of its unintended consequences.[101] As a result, FRT users are often either unaware or unconcerned that facial recognition can undermine free expression, free association, privacy, and anonymity, especially when used to target people at political events, protests, religious meetings, and other types of public gatherings where anonymity and the freedom to assemble are expected.[102]

In 2015, the United States Government Accountability Office ("GAO") issued a report warning that widespread and unregulated use of FRT could give businesses, government agencies, and even individuals the ability to identify (or misidentify) and track almost anyone in public without their knowledge or consent.[103] Just a few years later, there are multiple instances of the prophecy fulfilled: FRT company Clearview AI is facing a class action suit over its secret extraction and subsequent sale of individuals' photographs and biometric data;[104] cities like Chicago and Detroit have sophisticated surveillance networks running real-time facial recognition through hundreds of public and private cameras at parks, schools, churches, apartment buildings, and immigration centers;[105] and police investigators are manually editing low-quality and distorted photos in hopes of creating more matches and thus more arrests.[106]

There are many activities that require varying degrees of anonymity for people to freely participate and exercise their First Amendment rights. Political rallies, street protests, and houses of worship usually offer a measure

---

v. Postmaster Gen., 381 U.S. 301, 302, 307 (1965) (finding unconstitutional a statute preventing the U.S. Postal Service from delivering "communist political propaganda" to addressees unless they request to receive it, because it serves as a deterrent due to the sensitive nature of the material).

[100] *See* Talley v. California, 362 U.S. 60, 64 (1960) (holding that an ordinance barring the anonymous distribution of handbills restricts the freedom of expression and is thus unconstitutional); *see also* NAACP v. Alabama, 357 U.S. 449, 466 (1958) (finding Alabama's ban on the activities of NAACP lawyers and its demand to see the group's membership lists a violation of the members' rights to pursue their interests privately and to associate freely with others).

[101] *See Impact Hearing*, *supra* note 21, at 27 (testimony by Dr. Cedric Alexander).

[102] *See* Solon, *supra* note 21.

[103] *See GAO Report, supra* note 8, at 13, 17.

[104] *See* Bott, *supra* note 84.

[105] See *Impact Hearing*, *supra* note 21, at 1–2 (statement of Rep. Rashida Tlaib).

[106] *See* Drew Harwell, *Police Have Used Celebrity Look-Alikes, Distorted Images to Boost Facial-Recognition Results, Research Finds*, WASH. POST (May 16, 2019 6:12 PM), https://www.washingtonpost.com/technology/2019/05/16/police-have-used-celebrity-lookalikes-distorted-images-boost-facial-recognition-results-research-finds/ [hereinafter Harwell, *Police Have Used Celebrity Look-Alikes*].

of inconspicuousness for participants to feel comfortable.[107] Other activities may require total anonymity for participation to occur, such as visiting a medical center, or meeting with a media outlet when the individual is a whistleblower.[108] As surveillance networks grow and more and more persons become aware that they may be identified in public settings, some may instinctively, or purposefully, begin to avoid visiting or gathering in certain locations and events, which civil liberties groups contend is the chilling effect that makes this use of FRT a violation of their rights.[109] Moreover, the public is increasingly understanding that FRT users amass astonishing amounts of data considered private or sensitive, with no legal requirements to disclose their use of it or to dispose of it in any way.[110] This too can contribute to self-censorship and inhibition.

4. Civil Rights: The Disparate Effects of Facial Recognition

Of particular concern to rights advocates is the disproportionate effect FRT has on communities of color and poor communities, especially since law enforcement has a verifiable history of targeting activists and marginalized communities for surveillance.[111] First, various studies have shown that the technology is still considerably less accurate on certain groups, such as women and people of color.[112] African Americans, Asians, and Native Americans are up to one hundred times more likely to be misidentified by FRT as compared to white men, a potentially devastating discrepancy considering police investigators mostly use FRT to identify criminal suspects.[113] Studies conducted by the National Institute of Standards and

---

[107] *See* Jake Laperruque, *Unmasking the Realities of Facial Recognition*, POGO (Dec. 5, 2018), https://www.pogo.org/analysis/2018/2/unmasking-the-realities-of-facial-recognition.

[108] *Id.*

[109] *See GAO Report, supra* note 8, at 14; *see also* Nakar & Greenbaum, *supra* note 3, at 115 ("Awareness that the Government may be watching chills associational and expressive freedoms."); K. Brown, *supra* note 29, at 434–35 ("People involuntarily experience 'selfcensorship and inhibition' in response to the feeling of being watched.").

[110] *See* ANGLIM, *supra* note 7, at 191 (describing how privacy groups and government agencies are publicly expressing the concerns over personal data gathering, sharing, and use without consumer consent); *see also* K. Brown, *supra* note 29, at 464 ("Currently, there are no laws requiring private entities to provide individuals with notice that they are collecting personal data using FRT, how long that data will be stored, whether and how it will be shared, or how it will be used."); Wolfson, *supra* note 82, at 192 (noting that media sources worldwide are repeatedly informing the public of how their data is being processed and the associated dangers).

[111] *See* Kwet, *supra* note 4 (noting that law enforcement agencies have targeted marginalized communities for surveillance).

[112] *See Impact Hearing*, *supra* note 21, at 10 (statement of Neema Singh Guliani).

[113] *See* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition*

Technology ("NIST"), which develops standards for new technology, also continue to show higher error rates in determining a person's gender, age, or race,[114] despite developers' acknowledgment of the problem and assertions that steps are being taken to correct it.[115]

Another concern is that FRT disproportionately harms minority and marginalized communities.[116] This occurs because these communities tend to be over-policed, resulting in disproportionately high arrest rates.[117] This in turn leads to African Americans being over-represented in mug shots and disproportionately subjected to facial recognition searches by the police.[118] Despite these disparities, there is still no independent testing nor standardized internal testing for the aforementioned error rates.[119] In addition, the use of FRT in certain processes, such as jury selection at a trial, can negatively impact individuals by yielding results based on potentially discriminatory assumptions of demographic groups.[120] For example, facial recognition programs analyze and interpret facial expressions while at the same time scraping data about the potential jurors from public records and social media platforms.[121] Some programs then cross reference that data with assumptions about specific groups of people, such as Asian and Latin Americans having leadership skills– precisely the kinds of propensity notions lawyers are not

---

Systems, Casts Doubt On Their Expanding Use, WASH. POST (Dec. 19, 2019 6:43 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ [hereinafter Harwell, *Federal Study*].

[114] *See* Harwell, *Federal Study*, *supra* note 114.

[115] *See* ANGLIM, *supra* note 7, at 190 (noting that FRT error rates continue to decline even as the technology improves); *see also* Smith, *supra* note 36 (acknowledging the demographic differentials in FRT).

[116] See *Impact Hearing*, *supra* note 21, at 10 (statement of Neema Singh Guliani).

[117] *See Transparency Hearings*, *supra* note 10, at 32 (statement of Rep. Eleanor Holmes Norton).

[118] *See* Solon, *supra* note 21 (noting the disproportionality of African Americans who are subjected to police facial recognition); *see also Transparency Hearings*, *supra* note 10, at 32 (statement of Rep. Eleanor Holmes Norton - describing the excessive policing of minority communities and that it leads to a higher number of mug shots of African Americans).

[119] *See* Garvie, Bedoya, & Frankle, *supra* note 66; *see also* Solon, *supra* note 21 (relating that the Government Accountability Office has noted concern over the FBI's assessment of its FRT accuracy, and its lack of testing for false positives or racial bias).

[120] *See* Todd Feathers, *This Company Is Using Racially-Biased Algorithms to Select Jurors*, VICE (Mar. 3, 2020, 1:00 PM), https://www-vice-com.cdn.ampproject.org/c/s/www.vice.com/amp/en_us/article/epgmbw/this-company-is-using-racially-biased-algorithms-to-select-jurors.

[121] *See* Gabrielle Orum Hernández, *Facial Recognition Technology Used in Jury Consulting*, LAW.COM (Apr. 17, 2017 4:41 PM), https://www.law.com/sites/almstaff/2017/04/17/facial-recognition-technology-used-in-jury-consulting/ (describing facial recognition programs created to aid in the jury selection process).

allowed to weigh in *voir dire*.[122] Because the program considers race or gender-based propensity arguments to reach conclusions on the most favorable jurors, some rights advocates explain this could essentially be "tech-washing [people's] racialized assumption of individuals," but without transparency from the developer it cannot be known for sure.[123] And limiting the potential for harm, they contend, should not be left "to the good will of the agencies that procure [FRT], the corporations that develop [it], nor their secretive ethics departments . . . ."[124]

5. The Potential for Abuse

Equally troubling for rights advocates is the potential for abuse. The FRT industry lacks the transparency, guidelines, and safeguards necessary to ensure it is not misused in error, or exploited in malice.[125] There are no reporting requirements FRT providers or government entities must comply with that would inform the public when and how the technology is being used, nor is there any guidance or oversight on its use.[126] The public is forced to simply trust the FRT handlers with their biometric data.[127] However, the growing number of scandals involving mismanagement of private data, combined with reports detailing the questionable ways the technology is being employed, highlight the risk of misuse by good and bad actors alike.[128]

---

[122]U.S. Patent Application No. 20,190,130,778, col. 2 sec. 0074–75 (available at http://www.freepatentsonline.com/20190130778.pdf). The patent is for Momus Analytics, a jury selection software that uses biometric data including FRT to aid lawyers in discerning which jurors could be most influential during deliberations. Momus uses some race-based propensity arguments, such as leadership being a likely trait for people of Asian, Central American, or South American descent, while people who describe their race as "other" are less likely to be leaders.; *see also* Feathers, *supra* note 121 (noting the existence of certain stereotypes such as the notion that Black jurors are more sympathetic than white ones, and how it can lead to underrepresentation in jury panels).

[123] *See* Feathers, *supra* note 121 (quoting Gonzaga University professor Drew Simshaw, who studies artificial intelligence and legal technology: "[W]e don't know if the data that's being used is relying on data that reflects inequality, prejudice, and discrimination in society. The proprietary nature of the services, the lack of transparency, and this black box issue present challenges.").

[124] *See* Cuthbertson, *supra* note 90.

[125]*Impact Hearing*, *supra* note 20, at 9 (giving the statement of Neema Singh Guliani).

[126] *See* Pangburn, *supra* note 26 (noting the lax regulations, weak government oversight, and lack of clear rules or guidelines with regard to FRT).

[127] *See* YUE LIU, *supra* note 23, at 74 (detailing how businesses and government agencies do not offer any way for people to verify their data is being used in the manner they claim).

[128] *See* Giles & Deera, *supra* note 84 (listing the scandals surrounding the mishandling of user data by TikTok, Google, and Facebook); *see also* Harwell, *Police Have Used Celebrity Look-Alikes*, *supra* note 106 (noting some unethical uses of FRT to apprehend criminal suspects, such as using altered photos, composite sketches, and celebrity shots when the

In Florida, for example, the Pinellas County Sheriff's Office runs a program it makes available to all Florida law enforcement agencies which allows them to search through thirty-three million driver-license and police photos.[129] There are no requirements of reasonable suspicion to run a search, and no requirement to disclose the use of FRT[130] in *Brady* evidence.[131] Meanwhile, apartment complexes are starting to use FRT to grant access to individuals as well as to "enhance security,"[132] which many residents find invasive and impractical given the issues with the technology and the way it is being used.[133] The use of FRT for these purposes gives the user a powerful control tool that, when used improperly, can restrict an individual's freedom and self-development.[134]

III. PAST LEGAL RESPONSES AND CONDITIONING FACTORS

A. GDPR: The Response Abroad

In the 1990s, the emerging digital revolution took the world by storm, and the late 1990s saw the commercialism of FRT.[135] European lawmakers passed an EU Directive[136] to govern such emerging technologies and activity, but these policies were unable to keep up with the breadth and speed of the

---

suspect's photo was incomplete or distorted).

[129] *See* Karen Gullo & 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.

[130] *See* Garvie, Bedoya, & Frankle, *supra* note 65 (explaining how no state has yet passed laws that regulate police face recognition technology, nor has any state passed laws requiring the disclosure of facial recognition evidence to defense counsel).

[131] *See* Gullo & Lynch, *supra* note 129 (explaining that *Brady* evidence is information that could exonerate a defendant, such as knowing that the defendant was identified using a flawed process involving error-prone technology such as FRT).

[132] *See* Paris Martineau, *Cities Examine Proper—and Improper—Uses of Facial Recognition*, WIRED (Oct. 11, 2019 10:05 AM) https://www.wired.com/story/cities-examine-proper-improper-facial-recognition/ (describing the FRT currently deployed at a Manhattan apartment building and the push to install a FRT system at a Brooklyn, New York complex).

[133] *See* Martineau, *supra* note 132 (relating the reasons residents fought the implementation of FRT at their Brooklyn complex: it was often inaccurate, and it amounted to tenant harassment and an "extreme invasion of privacy").

[134] K. Brown, *supra* note 28, at 435.

[135] *Privacy and Civil Liberties Hearing, supra* note 5, at 14.

[136] *The History of the General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR (last visited Apr. 21, 2020), https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

revolution.[137] With the technological advancements came cyber threats, revelations by rogue insiders on the secret and often unethical manner in which state and private actors were gathering and using our data, and demands by private citizens to own and control their personal data.[138]

The European Union ("EU") recognizes data protection as a basic human right, as set out in Article 8 of the Charter of Fundamental Human Rights of the European Union.[139] Since the Charter's passing in 2000, the EU has steadily moved toward increased privacy protection and individual rights over personal data, and in 2016 it passed the General Data Protection Regulation ("GDPR"), which established uniform laws protecting consumer data and regulating its handling by any corporation who engages European citizens.[140] Thus, its effect is global because non-EU entities wishing to engage Europeans must abide by the GDPR.[141] Moreover, the GDPR applies when data is processed on equipment located in the EU, which prevents businesses from utilizing non-EU entities to sidestep the law.[142]

The GDPR qualifies biometrics as a special category of personal data, defining it as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[143] Recognizing the value of facial features because they are unique to an individual, it limits how organizations collect and use video surveillance and faceprints used for access control.[144] GDPR additionally requires data holders to employ cybersecurity controls to ensure that access to data is available only to those authorized to view it.[145] Finally, the GDPR requires an individual's active

---

[137] *See* Jocelyn Kryslik, *How the Evolution of Cybersecurity Has Led to GDPR*, BOBS GUIDE (Apr. 11, 2017), https://www.bobsguide.com/guide/news/2017/Apr/10/how-the-evolution-of-cybersecurity-has-led-to-gdpr/.

[138] *Id.*

[139] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, OCT. 26, 2012, 2012 O.J. (C 326) 391.

[140] *See* Carla Llaneza, *An Analysis on Biometric Privacy Data Regulation: A Pivot Towards Legislation Which Supports the Individual Consumer's Privacy Rights in Spite of Corporate Protections*, 32 ST. THOMAS L. REV. 177, 191 (2019).

[141] *Id.* at 191.

[142] W. GREGORY VOSS & KATHERINE WOODCOCK, NAVIGATING EU PRIVACY AND DATA PROTECTION LAWS 28 (A.B.A. Book Publishing ed., 2015).

[143] Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 34 [hereinafter GDPR].

[144] Mohammed Murad, *How Biometrics Complement GDPR Regulations,* IRIS ID (June 3, 2019), https://www.irisid.com/home-biometrics-complement-gdpr-regulations/.

[145] *Id.*

consent before a company can use his data.[146] The data must be collected and retained for specific and legitimate purposes, and must not be further processed in any way that is incompatible with either the specified purpose or the collection of the data.[147] Non-compliance can result in gargantuan penalties: up to €20 million or 4 percent of a company's annual worldwide revenue, whichever is greater.[148] By early 2020, 160,921 data breaches had been reported, with violators paying $126 million in fines.[149] Although significant, many in the EU believe these figures reflect "spotty enforcement" and "underwhelming fines,"[150] an indication Europeans will continue to enforce the GDPR, and eventually step up the penalties.

B. U.S. Regulations: The Response at Home

1. The Federal Level

The United States has no equivalent for some of the key EU regulations regarding data privacy.[151] The GDPR has, for all twenty-seven EU member states, strengthened privacy laws, recognized biometrics as protectible personal data, and enforced compliance.[152] Meanwhile, the U.S. federal government has engaged in what can be described as reactionary legislation, laws meant to address specific circumstances that have arisen with the proliferation of technology. For example, the Driver's Privacy Protection Act of 1994 restricts the sale of driver license photos to private parties, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 regulates the use and disclosure of an individual's health information, and the Gramm-Leach-Bliley Act of 1999, amended in 2015, restricts financial institutions' ability to share personal data.[153] However, the GAO has noted that none of these or other federal laws address biometric data broadly.[154] As a result, the laws do not extend to face recognition, nor can they extend to

---

[146] Llaneza, *supra* note 140, at 192.
[147] VOSS & WOODCOCK, *supra* note 142, at 17–18.
[148] Murad, *supra* note 144.
[149] Scott Ikeda, *GDPR Fines Top $126 Million With Over 160,000 Data Breaches Reported*, CPO MAGAZINE (Feb. 3, 2020), https://www.cpomagazine.com/data-protection/gdpr-fines-top-126-million-with-over-160000-data-breaches-reported/.
[150] *Id.*
[151] FEN OSLER HAMPSON & ERIC JARDINE, LOOK WHO'S WATCHING: SURVEILLANCE, TREACHERY, AND TRUST ONLINE 129 (Centre for International Governance Innovation ed., 2016).
[152] Kelly A. Wong, *The Face-Id Revolution: The Balance Between Pro-market and Pro-Consumer Biometric Privacy Regulation*, 20 J. HIGH TECH. L. 229, 258 (2020).
[153] *GAO Report, supra* note 7, at 33.
[154] *Id.*

circumstances other than those explicitly covered by each law.[155]

The Federal Trade Commission ("FTC") has in recent years begun flexing its regulatory muscle in response to a string of data breach and misuse scandals. For example, in 2019 alone, the FTC was instrumental in securing a $700 million settlement from Equifax, a $136 million penalty against Google and a YouTube subsidiary, and a record $5 billion penalty against Facebook– the largest ever in U.S history, representing a whopping 23% of Facebook's 2018 profits.[156] In addition to the fine, Facebook was required to take specific measures to avoid future incidents, such as setting up higher-level oversight and submitting to more stringent audits.[157] Although high penalties and forced measures are generally good deterrents for improper corporate behavior, absent clear guidelines, there is still much controversy over what constitutes improper handling of biometric data.[158]

2. Cities and Agencies Rejecting Facial Recognition Technology

As more is learned about the scope of FRT and its potential for exploitation by unregulated interests, some government agencies and U.S. cities have chosen to ban the technology altogether in the absence of any realistic hope Congress will pass comprehensive legislation in the near future that either bans or curtails the technology.[159] San Francisco, Oakland, Portland, Berkeley, and the Boston suburbs of Somerville and Brookline have banned FRT.[160] Police departments and cities across the country are debating the merits and concerns of the technology and considering similar bans.[161]

---

[155] *Id.*

[156] *See* Allison Grande, *The Biggest Privacy & Cybersecurity Developments of 2019*, LAW360 (Dec. 20, 2019, 1:25 PM), https://www.law360.com/articles/1228763/the-biggest-privacy-cybersecurity-developments-of-2019 [hereinafter Grande, *The Biggest Privacy*] (touching on some of the most notable data breach cases of 2019); *see also* Allison Grande, *FTC, Facebook Say $5B Privacy Deal Benefits Consumers*, LAW360 (Jan. 27, 2020, 8:58 PM EST), https://www.law360.com/articles/1237786/ftc-facebook-say-5b-privacy-deal-benefits-consumers [hereinafter Grande, *FTC*] (noting the details of the deal reached between the FTC and Facebook).

[157] *See* Grande, *FTC*, *supra* note 156.

[158] *See GAO Report, supra* note 7, at *Preface* (noting the disagreement amongst stakeholders on what risks FRT presents and whether the loss of privacy is offset by its benefits).

[159] *See* Matt O'Brien, *Why Some Cities, States and Lawmakers Want to Curb Facial Recognition Technology*, USA TODAY (Dec. 17, 2019 6:56 PM) https://www.usatoday.com/story/tech/2019/12/17/face-recognition-ban-some-cities-states-and-lawmakers-push-one/2680483001/.

[160] *Id.*; Rachel Metz, *Portland Passes Broadest Facial Recognition Ban in the US*, , CNN BUSINESS (Sept. 9, 2020 8:06 PM), https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.

[161] *See* O'Brien, *supra* note 159 (citing the city of Springfield, Massachusetts as one of the cities considering a ban on FRT).

California Governor Gavin Newsom signed a temporary moratorium on police department use of facial recognition with body cameras, mirroring similar restrictions in other states.[162] The concern over the civil liberties, privacy, and racial justice issues has even prompted FRT developers like Microsoft and Kairos to refuse to sell the technology to police agencies.[163]

3. State Privacy Legislation

In recent years, some states have begun enacting bills that address the management of biometric data including face recognition. The leader of this kind of legislation is undoubtedly Illinois, who in 2008 passed the Biometric Illinois Privacy Data Act ("BIPA")[164] which recognizes the unparalleled uniqueness of biometrics and the importance of protecting it from misuse.[165] BIPA defines biometric data as any information based on an individual's biometric identifier that is used for identification purposes, which would include facial recognition.[166] It outlines the proper collection, management, disclosure, and disposal of biometric data.[167] It sets out requirements for notifying individuals in writing and obtaining their consent prior to disclosure of their data to a third party.[168] Importantly, BIPA provides individuals with a private right of action, which allows any aggrieved party to sue for up to $1,000 per violation and $5,000 per intentional or reckless violation.[169] In 2019, the courts in a California case involving Facebook and an Illinois case involving Six Flags Entertainment determined that for purposes of Article III standing, any violation constitutes a cognizable and concrete injury-in-fact under BIPA.[170] The implications are astounding: anyone can bring suit as soon as there is a violation of BIPA.[171] Since these rulings, cases brought

---

[162] *Id.*

[163] *See id* (discussing Microsoft President Brad Smith's refusal to equip a California police department's squad cars and body cameras with its facial recognition software); *see also* Solon, *supra* note 20 (explaining that FRT developer Kairos has refused to provide the government with its software over concerns about biometric surveillance).

[164] 740 Ill. Comp. Stat. 14/1 et seq.

[165] Wong, *supra* note 152, at 238.

[166] 740 Ill. Comp. Stat. 14/10.

[167] Wong, *supra* note 152, at 240.

[168] *Id.* at 261.

[169] Llaneza, *supra* note 140, at 181–82.

[170] Jeffrey Rosenthal & David Oberly, *Biometric Privacy In 2020: What Companies Can Expect*, LAW360 (Feb. 4, 2020, 2:23 PM), https://www.law360.com/articles/1240262/biometric-privacy-in-2020-what-companies-can-expect- [Rosenthal & Oberly, *What Companies Can Expect*].

[171] *See* Mark A. Olthoff, Russell S. Jones Jr., & Elizabeth M. Marden, *Facebook "Tagged" in Certified Facial Scanning Class Action*, NAT'L L. REV. (Aug. 28, 2019) https://www.natlawreview.com/article/facebook-tagged-certified-facial-scanning-class-

under BIPA have multiplied, with payouts ranging from $80 to $1,300 per member in class action lawsuits.[172] Facebook was forced to settle for $650 million,[173] and other companies could potentially face large settlements unless they bring their practices into compliance with BIPA.[174] Thus, Illinois' powerful biometric privacy legislation has set the bar for other U.S. states to follow.[175]

Other states enacted biometric privacy laws early on, but none as comprehensive and consumer-friendly as Illinois. Texas passed the Capture or Use of Biometric Identifiers (CUBI) legislation shortly after BIPA went into effect.[176] Although it closely mirrors BIPA, it lacks the same teeth: it fails to define biometric information (much less mention facial recognition), and despite requiring notice and consent prior to biometric data being used for commercial purposes, it fails to define "commercial purposes."[177] While Washington state in 2017 passed H.B. 1493 restricting the commercial use of biometric identifiers, the legislation is seen as a business-friendly version of BIPA due to more relaxed regulations regarding the manner in which data is gathered or subsequently used, and the fact that notification and consent are not always mandatory.[178] Furthermore, both Washington and Texas bypassed the private right of action, leaving litigation in the hands of the state

---

action (discussing the Ninth Circuit Court of Appeals ruling holding that mere collection of a person's biometric data without his or her consent constituted real or threatened injury under BIPA).

[172] *See* Richard R. Winter, Rachel C. Agius, William F. Farley, *BIPA Update: Class Actions on the Rise in Illinois Courts*, HOLLAND & KNIGHT (July 22, 2019), https://www.hklaw.com/en/insights/publications/2019/07/bipa-update-class-actions-on-the-rise-in-illinois-courts.

[173] Malathi Nayak, *Facebook Sweetens Biometric Privacy Accord to $650 Million*, BLOOMBERG (July 23, 2020, 4:55 PM), https://www.bloomberg.com/news/articles/2020-07-23/facebook-proposes-650-million-to-settle-biometric-privacy-case.

[174] *See* Rosenthal & Oberly, *What Companies Can Expect*, *supra* note 170 (explaining that the Facebook and Rosenbach rulings have "opened the floodgates to a new wave of extremely costly litigation . . . ").

[175] *See* Allison Grande & Ben Kochman, *BIPA Bares Its Teeth in Facebook Biometric Privacy Deal*, LAW360 (Jan. 30, 2020 10:39 PM), https://www.law360.com/articles/1239383/bipa-bares-its-teeth-in-facebook-biometric-privacy-deal (citing the Facebook $550 million settlement as a key test proving the unique power of BIPA).

[176] Tex. Bus. & Com. Code Ann. §503.00.

[177] *See* Llaneza, *supra* note 140, at 10.

[178] *See* Wong, *supra* note 152, at 242–44 (detailing the reasons H.B. 1493 is viewed as business-friendly, among them the fact that "a person is not obligated to provide notice nor obtain consent for biometric identifiers that are merely captured, collected, or enrolled in furtherance of a security purpose, or in the alternative, are merely captured for a commercial purpose.").

attorney general.[179]

The only state to enact biometric privacy laws rivaling the scope and force of BIPA is California, which passed the California Consumer Privacy Act ("CCPA") that went into effect in January 2020.[180] Taking its cue from the GDPR, the CCPA gives California residents broad rights over their biometric data. It generally lays out strict guidelines requiring companies to be transparent about the personal data collected and how it is disclosed or shared; it gives consumers control over how their data is sold or shared, as well as the option to have it deleted; and it requires websites to have clear and conspicuous "opt out" options for consumers not wishing their personal data to be monetized.[181] Furthermore, the CCPA creates a private right of action like BIPA, and currently serves as a landmark law that puts pressure on the U.S. Congress to enact legislation that protects Americans' data privacy rights.[182]

In November 2020, California passed the California Privacy Rights Act (CPRA), which amends and supersedes the CCPA.[183] Set to become effective on January 1, 2023, the CPRA expands the framework of the CCPA in several important ways that will directly impact the use of FRT.[184] For example, it defines a new subcategory of "sensitive" personal information ("Sensitive PI") such as biometric and genetic information, the processing of which Californians will have greater control over.[185] The CPRA also makes businesses more accountable to consumers with regard to the use of their Sensitive PI.[186] Furthermore, the CPRA gives consumers the power to partially limit profiling, defined as the automated processing of personal information in order to "analyze or predict aspects of a person's preferences, economic situation, work performance, health, interests, behavior, location,

---

[179] *See* Llaneza, *supra* note 140, at 12.

[180] Cal Civ Code Div. 3, Pt. 4, Title 1.81.5.

[181] *See California Consumer Privacy Act: A Reference Guide for Compliance*, J.D. SUPRA 3 (Oct. 22, 2019) https://www.jdsupra.com/legalnews/california-consumer-privacy-act-a-94563/.

[182] *See* Llaneza, *supra* note 140, at 15.

[183] *See* Brandon P. Reilly and Scott T. Lashway, *The California Privacy Rights Act Has Passed: What's in It?*, MANATT (Nov. 11, 2020) https://www.manatt.com/insights/newsletters/client-alert/the-california-privacy-rights-act-has-passed (describing the passage of the CPRA).

[184] *See* Michael Bahar, Mary Jane Wilson-Bilik and Alexander F. L. Sand, *California's New Privacy Law, the CPRA, Was Approved: Now What?*, LEXOLOGY (Nov. 9, 2020) https://www.lexology.com/library/detail.aspx?g=5a7edce9-26af-487c-8877-7a815945954d [hereinafter *California's New Privacy Law*].

[185] *See* Reilly & Lashway, *supra* note 183 (explaining that under the CPRA, consumers will have a new right to restrict the use and disclosure of Sensitive PI).

[186] *See California's New Privacy Law*, *supra* note 184 (describing the requirements that businesses limit and disclose the use and retention of Sensitive PI).

reliability, or movements."[187] FRT users who fail to comply with the new regulations will have to contend with the newly created California Privacy Protection Agency (CPPA), which has investigative, enforcement, and rulemaking powers.[188] These as well as other new, robust measures make the CPRA the likely precursor to future federal privacy legislation in the U.S.[189]

IV. FUTURE TRENDS

A. How FRT Will Be Used

FRT supporters continue to find new uses for facial recognition, pushing the envelope and delving into areas unknown. Facebook, for example, has applied for patents that would allow its FRT to detect customers in physical stores and match them to their social networking profiles.[190] And the technology is being used in Denmark soccer stadiums to fight hooliganism: thousands of soccer match attendees have their faces scanned and compared against a list of banned troublemakers who are denied entrance.[191] In order to not run afoul of the GDPR, authorities run the system only on game days and not on the Internet, and the data, which is cross-checked to avoid false positives, is deleted at the end of the day.[192] A soccer fan's opinion of the new security measure echoes the opinion held by many: "Facial recognition is inevitable."[193]

In America, this idea of the inevitability of FRT can be traced to the 9/11 terror attacks. Although FRT had been used for commercial as well as security purposes, the attacks pushed facial recognition to the forefront of the biometrics industry as the government sought new counterterrorism strategies.[194] Americans seemed to accept this "new" technology that invaded their privacy somewhat in exchange for increased national

---

[187] *See id.* (discussing the new definition of and restrictions on "profiling").

[188] *See* Gretchen A. Ramos, *CPRA Favored by California Voters – Practical Takeaways*, NAT'L L. REV. (Nov. 4, 2020) https://www.natlawreview.com/article/cpra-favored-california-voters-practical-takeaways?utm_content=8d9aba66946c2bd8f122f21c6d39f01a&utm_campaign=2020-11-5Cybersecurity%20Legal%20News&utm_source=Robly.com&utm_medium=email.

[189] *See id.*

[190] Singer, *supra* note 42.

[191] Sidsel Overgaard, *A Soccer Team in Denmark Is Using Facial Recognition to Stop Unruly Fans*, N.P.R. (Oct. 21, 2019 5:39 PM) https://www.npr.org/2019/10/21/770280447/a-soccer-team-in-denmark-is-using-facial-recognition-to-stop-unruly-fans.

[192] *Id.*

[193] *Id.*

[194] *See* JEFFERSON, *supra* note 65, at 72 (describing the emphasis on developing FRT after 9/11).

security.[195] Almost twenty years later, even though facial recognition is being used across many industries and for a variety of purposes, the increasing demand by government and private organizations for its use in surveillance systems is said to be driving the market.[196] Despite the concerns, FRT providers and consumers alike extol the virtues of the technology in programs that help keep our borders and citizens safe.[197]

The TSA's 2018 Biometrics Roadmap is one example, a pilot project carried out in collaboration with CBP to check international travelers' biometrics.[198] Officials contend that the technology has given them the ability to identify more than 14,000 aliens who have overstayed their visas, as well as to identify more than 130 individuals attempting to enter the country with false documents.[199] Even though rights activists denounce such unfettered access to all of a person's data, including images and contact information,[200] organizations will continue, in the name of public safety, to employ FRT in increasingly innovative ways.

There is a logical belief that widespread use of facial coverings during a pandemic like COVID-19 would thwart FRT algorithms and lead to a decline in its use.[201] However, FRT developers have found ways to adapt their technology and are working overtime to improve the accuracy of partially covered faces.[202] In addition, the ability to identify masked personnel from a distance has become crucial to places needing to enable contactless security

---

[195] *See* ANGLIM, *supra* note 7, at 191 (noting that consumers willingly exchange some privacy for the security surveillance technology provides).

[196] *See* Nakar & Greenbaum, *supra* note 3, at 96 ("FRT is already implemented in many areas such as security, commerce, social media, personal use, and even for religious purposes."); *see also Facial Recognition Market to Hit $12 Billion, supra* note 47 ("Growing demand for surveillance systems drives the demand for the global facial recognition market.").

[197] *See supra* Section II.A.ii.

[198] See *Transparency Hearings*, *supra* note 10, at 3 (statement of Austin Gould) (describing the various goals of the Biometrics Roadmap).

[199] TSA BIOMETRIC REPORT, *supra* note 67, at 32.

[200] *See* K. Wehle, *supra* note 29, at 466 (speaking broadly to the need for constitutional regulation and oversight of FRT).

[201] *See* Hvistendahl and Biddle, *supra* note 25 (noting that the use of facial coverings has presented "an obvious roadblock" to the global expansion of FRT).

[202] *See generally* Rebecca Heilweil, *Masks Can Fool Facial Recognition Systems, but the Algorithms Are Learning Fast*, VOX (July 28, 2020 10:20 AM), https://www.vox.com/recode/2020/7/28/21340674/face-masks-facial-recognition-surveillance-nist (Describing the race between companies to update their FRT algorithms to account for masks); *see also* Susan Miller, *Facial Recognition Adapts to a Mask-Wearing Public*, GCN (June 3, 2020), https://gcn.com/articles/2020/06/03/facial-recognition-masks.aspx (describing how FRT providers across the world have been working for months to adapt their technology to recognize mask-wearers, including by adapting the technology to focus on the person's eyes).

and control, driving new demand for the technology.[203] For example, Chinese hospitals are already using FRT that identifies masked nurses –and can eventually check their temperatures– from several feet away at hospital entrances.[204] In Europe and the U.S., some employers have quietly started using advanced FRT to ensure their staff's compliance with mask requirements.[205] Given the magnitude of the COVID-19 pandemic and the expectation that more pandemics will occur,[206] it is not a stretch to imagine other types of employers using FRT to ensure that their essential personnel remain masked at all times.[207]

B. Rejection of FRT

Some FRT opponents reject the use of the technology in any application or measure, citing the abuse or potential for abuse due to indiscriminate use by businesses and government authorities.[208] While some major cities have banned its use outright and others consider partial or total bans,[209] some organizations have not waited for their local government to take action; instead, they have implemented their own ban on the use of FRT within their sphere. Several college campuses, for example, disavowed the use of the technology after being pressured by student advocates.[210] Concert promoter

---

[203] *See* Mark Rasdale, John Magee, Cezary Bicki, Eilís McDonald, Marlene Winther, Plas Emil Agerskov Thuesen & Carolyn Bigg, *Facial Recognition Technology: Supporting a Sustainable Lockdown Exit Strategy?*, DLA PIPER (May 8, 2020), https://www.dlapiper.com/en/us/insights/publications/2020/05/facial-recognition-technology/ (discussing an Irish food producer that implemented advanced FRT in order to make employee clock ins and security access contactless and germless).

[204] *See id.* (discussing the FRT being used in Chinese hospitals at the center of the COVID-19 outbreak).

[205] *See* Yan, *supra* note 25 (noting that restaurants, hotels, and at least one airport have begun using FRT to detect mask-wearing staff).

[206] *See* 9 Nita Madhav Et Al., Disease Control Priorities: Improving Health and Reducing Poverty 315 (Dean T. Jamison, et al. eds., 3rd ed. 2017), https://www.ncbi.nlm.nih.gov/books/NBK525289/pdf/Bookshelf_NBK525289.pdf (explaining that the likelihood of pandemics is growing due to an increase and intensification of contributing trends like global travel and integration, and urbanization).

[207] *See* Yan, *supra* note 25 (contending that more private organizations, such as department stores, could begin using FRT to detect mask-wearers).

[208] *See supra* Section III.B.ii.

[209] *See supra* Section III.B.ii; *see also* Douglas Hook, *Easthampton Passes Municipal Ban on Facial Recognition Tech*, BIZJOURNALS (July 2, 2020, 10:35 AM) https://www.bizjournals.com/boston/news/2020/07/02/easthampton-passes-ban-on-facial-recognition.html (noting Boston's ban on municipal use of facial recognition technology).

[210] *See* STOP FACIAL RECOGNITION ON CAMPUS, https://www.banfacialrecognition.com/campus/ (last visited Apr. 21, 2020) [hereinafter STOP FRT] (citing several schools such as Harvard University, Stanford University,

Live Nation has no plans to begin using it.[211] At least three major FRT developers have announced they will not allow their technology to be used by law enforcement,[212] and one big one –Amazon– faced pushback last year from its own shareholders when it began to market its facial recognition software to police departments.[213]

FRT providers have taken notice and have begun to call for national standards that would essentially restrict the use of FRT rather than outright ban it.[214] Microsoft, IBM, and Google have each called for such measures, saying the government must address the current debates so that individuals' rights are protected as the technology grows.[215] Analysts, however, believe this sudden interest in regulations is the industry's attempt to dissuade lawmakers from weighing an outright ban on the technology.[216] Tech firms would clearly prefer restrictions on FRT use to the types of prohibitions that some of the nation's major cities are considering.[217] Thus, industry clamor for regulations will likely continue, and based on the federal government's failure to enact legislation thus far, it is likely that states will continue to pass their own biometric data laws.

C. The Future of FRT Regulations in the U.S.

There is a clear trend toward state regulation of FRT where states are enacting new biometric privacy laws or expanding existing ones.[218] New York accomplished both in 2019 by passing its Stop Hacks and Improve Electronic Data Security ("SHIELD") Act; it expanded the definition of

---

Massachusetts Institute of Technology (MIT), and the University of California at Los Angeles (UCLA) that refuse to use facial recognition on their campuses).

[211] *See Biometrics Tech Firms Want Moderation, Not Bans, On Facial Recognition*, PYMNTS (Mar. 8, 2020), https://www.pymnts.com/news/biometrics/2020/tech-firms-want-moderation-not-bans-facial-recognition/.

[212] *See* sources cited *supra* note 164; *see also* Chappell, *supra* note 91 (noting that the largest manufacturer of police body cameras, Axon, declines to sell facial recognition technology).

[213] See *Impact Hearing*, *supra* note 21, at 10–11 (statement of Neema Singh Guliani).

[214] Ryan Tracy, *Tech Firms Seek to Head Off Bans on Facial Recognition*, WALL ST. J. (Mar. 8, 2020 4:32 PM), https://www.wsj.com/articles/tech-firms-seek-to-head-off-bans-on-facial-recognition-11583498034.

[215] *Biometric Tech Firms Want Moderation, Not Bans, On Facial Recognition*, *supra* note 212.

[216] *See* Kaveh Waddell, *IBM calls for regulation to avoid facial recognition bans*, AXIOS (Nov. 6, 2019), https://www.axios.com/ibm-facial-recognition-regulation-ban-50000b77-109d-4472-b4c5-316b858e7d74.html.

[217] *See* Tracy, *supra* note 215 (noting Microsoft's support of state and federal regulations but not bans).

[218] *The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020*, NAT'L. L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020 [hereinafter *Anatomy of Biometric Laws*].

personal information covered by current law to include biometric data, and it imposed new requirements for data security.[219] In 2019, some states passed targeted privacy legislation: Nevada's gave consumers the ability to opt out of the sale of their data, Maine's required the consumer's consent to use, share, or sell his or her personal data,[220] and Arkansas, California, and Washington each added biometric data to regulations requiring breach notifications.[221] Furthermore, several other states have introduced bills proposing either new legislation of biometric data or strengthening existing consumer protection laws that cover biometrics.[222] Thus, there will be a continued push for state biometric privacy laws to restrict the use of facial recognition.

The federal government has held several hearings in recent years on FRT, its use, its impact, and the need for national guidelines, an idea that enjoys bipartisan support.[223] A staunch conservative, House Representative Jim Jordan even said, "It doesn't matter if it's a President Trump rally or a Bernie Sanders rally, the idea of American citizens being tracked and cataloged for merely showing their faces in public is deeply troubling."[224] Last year, Congress introduced the Commercial Facial Recognition Privacy Act of 2019 ("CFRPA"),[225] which would require certain companies to obtain consent before using FRT to identify or track individuals, or sell their face data.[226] Later in the year, legislators weighed a prohibition on the sale of biometric data as part of the law.[227] Despite all the talk about the inaccuracy of FRT, especially with regard to people of color, and its unchecked and often secret use by government agencies and the private sector, the CFRPA has not made it to a vote.[228]

Another bipartisan bill, the Facial Recognition Technology Warrant Act of 2019,[229] was introduced in November 2019 and seeks to address the privacy and discrimination concerns of the federal government's use of

---

[219] Rosenthal & Oberly, *Legal Landscape*, *supra* note 28.
[220] Grande, *The Biggest Privacy*, *supra* note 157.
[221] Rosenthal & Oberly, *Legal Landscape*, *supra* note 28.
[222] Amanda Lawrence, Sasha Leonhardt & David Rivera, *State Privacy Law Initiatives to Prepare For In 2020*, LAW360 (Feb. 6, 2020 2:54 PM), https://www.law360.com/articles/1241213/state-privacy-law-initiatives-to-prepare-for-in-2020.
[223] *See* Johnson, *supra* note 11 (noting that the Congressional House Oversight and Reform Committee has held three hearings on FRT in the past year alone, and Democrats and Republicans agree on the need for federal oversight on FRT use).
[224] *Id.*.
[225] Commercial Facial Recognition Privacy Act of 2019, S.B. 847, 116th Cong. (2019).
[226] *Id.*
[227] Rosenthal & Oberly, *Legal Landscape*, *supra* note 28.
[228] *See* L. Brown, *supra* note 58.
[229] Facial Recognition Technology Warrant Act of 2019, S.B. 2878, 116th Cong. (2019).

FRT.[230] Under the Act, federal law enforcement authorities would need a probable cause warrant to use FRT to track an individual for longer than seventy-two hours, with a maximum of thirty days. In addition, it would require federal reporting on FRT use to the NIST to gauge and improve accuracy.[231] These provisions are seen as a middle ground of sorts that places limits on facial recognition while still allowing its use in certain cases involving security concerns.[232] The bill is currently pending the Senate Judiciary Committee.

V. ASSESSMENT OF PAST LEGAL RESPONSES; ALTERNATIVES; AND SOLUTIONS

A. Evaluation: What Works, What Doesn't

Proponents and opponents of FRT are increasingly beginning to agree that the lack of federal standards regarding FRT poses the greatest problem for the industry and the public alike. Despite multiple Congressional hearings on the matter and Congress's stated interest in defining biometric privacy laws for the nation, there seems to be disagreement as to whether federal law should always preempt state law in this area, how to enforce these laws, and whether consumers should have a private right of action to pursue litigation for violations.[233] A 2016 attempt to create the "best practices for the commercial use of FRT" failed when rights advocacy groups objected to the lack of an opt-in system for consumers.[234] And while states have been enacting and enforcing their own biometric privacy laws, the regulations differ on key issues, which means the protections consumers are afforded vary from state to state.[235] In addition, FRT supporters argue that the lack of uniformity in state biometrics regulations hinders innovation; businesses risk

---

[230] Chris Coons & Mike Lee, *Facial Recognition Technology Warrant Act Of 2019*, COONS (2019), https://www.coons.senate.gov/imo/media/doc/FRTWA%20One-Pager%20FinalFinal.pdf.

[231] *Id.*

[232] Caitlin Chin, *Highlights: Setting Guidelines for Facial Recognition and Law Enforcement*, BROOKINGS (Dec. 9, 2019), https://www.brookings.edu/blog/techtank/2019/12/09/highlights-setting-guidelines-for-facial-recognition-and-law-enforcement/.

[233] *See Impact Hearing*, *supra* note 20, at 28 (comments by Andrew G. Ferguson) (suggesting that the federal government should "set the floor" while state and local governments can create heightened standards); *see also* Rosenthal & Oberly, *Legal Landscape*, *supra* note 27 (discussing Congress' inability to pass FRT regulation despite several hearings and the introduction of bills focusing on different protections).

[234] *See* Nakar & Greenbaum, *supra* note 2, at 119–21 (describing the U.S. Department of Commerce's push in 2016 to release a set of guidelines for FRT use).

[235] *Supra* Section III.B.iii.

costly fines in the testing of new products and services across a market because they may be compliant in one state but not in another.[236] Thus, a national standard is needed.

Of the state legislative frameworks on which to base a national standard, California's CCPA and Illinois' BIPA seem to be the most comprehensive and forward-looking. The CCPA is practically a carbon copy of the GDPR, which is based on the premise that an individual is entitled to control over and protection of his personal data.[237] Due to the CCPA's precise definitions and guidelines, corporations for the most part have been forced to carefully craft their use of FRT and weigh its benefits against the risk of costly litigation and penalties (unlike the GDPR, there are no caps to CCPA fines and they are assessed per violation).[238] Additionally, the fact that the CCPA mirrors the EU's GDPR and is one of the more stringent of the biometric laws in the U.S., compliance with the CCPA often equals compliance with other privacy frameworks including the GDPR. Meanwhile, both the CCPA and BIPA grant consumers the right to bring a claim for violations, opening the door to class action lawsuits which are a powerful deterrent for the mishandling of FRT.

B. Alternatives: Keep the "Wild West" or Ban FRT?

Some proponents of FRT contend that the current federal regulatory environment (no regulations) is inherently the best situation for everyone. It allows the technology to continue to develop, resulting in the developers continuing to find breakthrough ways to employ it, and thereby the market continues to thrive to the tune of billions of dollars.[239] These supporters downplay the First Amendment and privacy rights concerns, suggesting that there is a powerful counter argument about what our expectation of privacy is nowadays, and that we continue to redraw the proverbial line in the sand as we find further positive uses for the technology outweighing the perceived negative consequences.[240] However, according to rights advocates, FRT,

---

[236] Wong, *supra* note 152, at 260.

[237] *See* Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in The UK*, WIRED (Mar. 24 2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (noting the similarity between the GDPR and the CCPA).

[238] Michael Fertik, *CCPA is a Win For Consumers, But Businesses Must Now Step Up On CX*, FORBES (Jan. 27, 2020 5:40 PM), https://www.forbes.com/sites/michaelfertik/2020/01/27/ccpa-is-a-win-for-consumers-but-businesses-must-now-step-up-on-cx/#68a34d3f6557.

[239] *See Facial Recognition Market to Hit $12 Billion, supra* note 46 (noting the expected growth in the facial recognition market); *see also* Coons & Lee, *supra* note 230 (explaining that an outright ban on FRT could discourage innovation).

[240] *See* K. Brown, *supra* note 28, at 416 (stating that people seem to willingly tolerate privacy

with no oversight in place and wielding the power to assemble sensitive or personal data about private persons,[241] in addition to violating constitutional rights, can be used to harass or even stalk individuals.[242] And as more businesses begin to employ FRT, this will lead to more private and public databases of information than can be shared, monetized, or even hacked and used by bad actors.[243] Therefore, maintaining the status quo is not in the best interest of the consumer or the public at large.

On the opposite end of the spectrum, the argument for a facial recognition moratorium is very much alive. Some feel its use should be halted while the government decides how best to move forward with regulation.[244] Others believe FRT should be suspended until the proper safeguards are actually implemented.[245] Still, others insist there is never a place for FRT in certain locations like college campuses, and urge its complete prohibition as the only way to truly stop the unconstitutional spying on Americans.[246] These advocates claim that judicial rejection of an expectation of privacy while in public, together with deficiencies in current regulations, allow FRT users to deploy the technology despite constitutional barriers.[247] For instance, under the third party doctrine, there is no Fourth Amendment ban on government use of personal data obtained through nongovernmental entities.[248] Thus, using a private business to collect the information allows law enforcement to sidestep the constitutional requirement to obtain a warrant prior to surveillance.[249]

However, many other individuals believe that there are legitimate commercial and law enforcement uses of facial recognition, and a ban could make citizens less safe, as well as discourage important innovation.[250] A

---

intrusions if they safeguard their well-being).

[241] Nakar & Greenbaum, *supra* note 2, at 115.

[242] Solon, *supra* note 20.

[243] *See* Wolfson, *supra* note 81, at 192 ("Data protection has become increasingly important because the development of technology has led to prevalent data collecting and processing in the public and private sectors.").

[244] *See Impact Hearing*, *supra* note 20, at 17 (comments by Andrew G. Ferguson); see also *Impact Hearing*, *supra* note 20, at 14 (statement by Neema Singh Guliani).

[245] ANGLIM, *supra* note 6, at 190.

[246] STOP FRT, *supra* note 210.

[247] *See* K. Brown, *supra* note 28, at 466 (describing how judicial rejection of a reasonable expectation of privacy plus the third party doctrine allows the government to surveil citizens despite constitutional barriers).

[248] *Id.* at 443, 466.

[249] *See id.* at 466 ("The third party doctrine and the longstanding judicial rejection of a reasonable expectation of privacy in matters made public have depleted the Fourth Amendment of vitality for purposes of establishing constitutional barriers to the government's use of FRT to profile and monitor individual citizens.").

[250] Chris Coons & Mike Lee, *supra* note 230.

2006 White House report noted:

> Government and industry have a common challenge in today's global society to provide more robust identity management tools, and identity governance principles on how to deploy these tools intelligently to meet national and international needs. Collaboration among the biometrics community–government, industry and academia–on these common challenges is essential.[251]

This view supports the idea that FRT providers and the government will each benefit if they endeavor to make facial recognition both more reliable and protective of individual rights.[252] One example of how this could work would be a provision requiring all FRT to be assessed for accuracy by a third party who would set the parameters and publicly release the results.[253] The federal government could also require their agencies use a facial recognition program that meets a minimum accuracy rate. Because of this requirement plus the public being informed of each provider's technology's accuracy and potential for unfair bias, market forces would drive sales of the higher quality software, forcing developers producing substandard technology to improve their product or be pushed out of the market. [254] Thus, an FRT provider outperforming the competition will be rewarded with increased sales figures, while the FRT users –and their subjects– are rewarded with reliable results and a reduced risk of racial bias.[255]

Another option for the future of FRT is to require that providers have consumers opt in or out of their services, which would force private organizations to disclose the kind of information they are collecting from consumers and how they plan to use it.[256] Google, for example, requires

---

[251] The National Biometrics Challenge, National Science and Technology Council Subcommittee on Biometrics, page 1, (Aug., 2006), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/biometrics_challenge_document.pdf.

[252] *See* HAMPSON & JARDINE, *supra* note 151, at 278 (stating that "new kinds of collaborative institutional arrangements" will help manage the evolution of data privacy laws); *see also* Smith, *supra* note 35 (proposing the government pass legislation that incentivizes the development of more accurate FRT).

[253] *See* Smith, *supra* note 35 (contending FRT should be tested for accuracy, in a transparent and even-handed manner, by impartial groups.).

[254] *Id.*

[255] *Id.*

[256] *See* HAMPSON & JARDINE, *supra* note 151, at 17 ("Private corporations must come out of the shadows, come clean about the information they are gathering from us when we use their products and services."); *see also* ANGLIM, *supra* note 6, at 192 ("Suggested best practices

consumers to turn on a "find my face" feature in their smartphones in order to enable facial recognition.[257] Other companies such as Microsoft and MasterCard require the user download software or purchase hardware.[258] Where facial recognition is used in a physical location such as a retail store or a bank, signs should be posted alerting the consumer as to what services will use their facial image should they choose to enter the premises.[259] When a consumer needing a service is forced to choose between surrendering his privacy or seeking that service from a competitor, his ultimate decision will shed light on his opinion of the technology and the importance of his consent. Regardless, consent is fundamental to respecting the rights of individuals over their biometric data, and it should be required in every commercial use of FRT.[260]

C. Solution: There is No One Solution

Ideally, FRT would be regulated under one set of national guidelines that supersedes individual state laws. However, any regulation, whether it be state or federal, should do more than just penalize certain uses of the technology; it should incentivize all stakeholders to view biometric data, the most reliable source of identification, as a precious commodity, inextricably intertwined with an individual's dignity.[261] As such, a faceprint should not be subjected to an unwarranted search and match, or storage in a database without the individual's consent, much less nonconsensual sale to a third party. Any thought to the contrary would mean people would be forced to hide their faces in public spaces in order to prevent government and commercial tracking, as well as the trafficking of their personal data. Striking the right balance so that government and business interests do not infringe on political freedoms and civil liberties is perhaps the greatest challenge the U.S. and other democratic societies face today.[262] Many fundamental human values reside at this crossroads: power, wealth, ethics, respect, knowledge, and the maximization of skills are all in play.[263]

[for commercial FRT use] vary, but most call for disclosing the technology's use and obtaining consent before using it to identify someone from anonymous images.").

[257] ANGLIM, *supra* note 6, at 193.

[258] *Id.*

[259] Smith, *supra* note 35.

[260] *See supra* Section II.B.i.

[261] *See* Neo Sesinye, *Know the value of your digital and biometric data*, IT NEWS AFRICA (Mar. 4, 2019), https://www.itnewsafrica.com/2019/03/know-the-value-of-your-digital-and-biometric-data/ (emphasizing the value of biometric data, and that it is "paramount and therefore deserves the utmost respect and protection").

[262] GUIORA, *supra* note 26, at 77.

[263] Siegfried Wiessner, *The New Haven School of Jurisprudence: A Universal Toolkit for*

1. How Much Is It Worth?

The first step in restoring order to this "wild west" is to properly monetize biometric data, and specifically facial recognition data. This kind of data holds massive value for entities needing to quickly verify individuals attempting to use their service; its authenticity is relied upon to seek out persons of interest, to verify the recipient of a bank wire transfer, or to authorize access to a secure device or space, among the many uses.[264] In addition, commercial enterprises whose business is based upon Internet commerce depend on the value of intangible assets, such as large consumer databases, to adequately exploit their organization's market value, to secure financing, and even turn a relatively easy net profit on a sale to a third party.[265] A clear example of personal data being monetized by the holder (as opposed to the individual) is the post-bankruptcy sale of retailer Sports Authority's customer database for $15 million.[266] If companies use people's biometric data for financial gain, then the data owners must be compensated.[267]

An individual's faceprint should have a real value, even a dollar value, and this should belong to the individual if she chooses to allow the use of her image.[268] Without faceprints, FRT companies are unable to test and continually improve their technology.[269] In addition, companies such as retailers are using these images to make money, images acquired without the persons' knowledge and at basically no cost other than the initial purchase of the facial recognition software.[270] Around 2.5 billion photos are uploaded to Facebook alone every month. So long as FRT users are allowed to sell those images without consumer knowledge, consent, or compensation, the low cost

---

Understanding and Shaping the Law, 81 ASIA PACIFIC L. REV. 45, 51–52 (2010).

[264] *See supra* Section I.A.

[265] Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 428 (2018) [hereinafter Elvy, *Commodifying Consumer Data*].

[266] *Id.* at 431.

[267] *See* Solon, *supra* note 20 (arguing that strict rules on FRT are especially applicable when private organizations collect and utilize a great number of facial images).

[268] *See generally* Magali Eben, *Market Definition and Free Online Services: The Prospect of Personal Data as Price*, 14 I/S: J. L. & POL'Y FOR INFO. SOC'Y 227 (2018) (proposing that personal data can be monetized and traded for services).

[269] Lafrance, *supra* note 32.

[270] *See Privacy and Civil Liberties Hearing, supra* note 5, at 9 (statement of Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, Federal Trade Commission, stating that the rapid growth in the availability of online photos means companies do not need to purchase identified images, which lowers costs and makes facial recognition technologies commercially viable for many organizations).

and potential profit will remain too seductive a practice to discontinue.[271] Thus, any law addressing the commercial use of facial recognition should have a provision requiring the data initially be acquired from the individual by purchase and with consent.

Attempts have been made to translate this idea to dollars and cents.[272] In 2014, New York-based company Datacoup began compensating persons for their personal data, in hopes of creating a marketplace for businesses to purchase personal data obtained directly from the consumer.[273] Datacoup may have been ahead of its time; "big data" competitors, able to scour the Internet and scrape massive amounts of personal information (without consumer consent), offered bigger pools of data to Datacoup's clients, and at a lower cost, eventually helping to bring about the company's demise in 2019.[274] Had there been federal laws prohibiting the scraping of people's social media pages and online activity for the nonconsensual monetization of their private data, Datacoup might today be the pioneer of a verdant and equitable marketplace of personal data, including biometrics.

There have been other attempts to monetize personal data.[275] In a privacy-discount program, a company grants consumers a discount on services they are purchasing in exchange for the ability to use their personal data.[276] For example, Internet Service Provider AT&T once offered a $30 discount on its broadband service to customers who consented to the sharing of their browsing data for things like targeted ads.[277] The concept is on point: the consumer is offered monetary value for his personal data, and he is free to decide if he accepts the exchange. It would be up to regulations requiring transparency among other things, to ensure companies do not artificially

---

[271] *Id.* at 9 (statement of Maneesha Mithal) (explaining that FRT is a viable commercial option for many companies because there is no need to purchase the images, which keeps costs low).

[272] *See* Eben, *supra* note 268, at 267–68 (noting companies Datacoup and People.io who offered monetary compensation, discounts, and free goods for their customers' personal data).

[273] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1398 (2017) [hereinafter Elvy, *Paying for Privacy*].

[274] *Datacoup*, WIKIPEDIA, https://en.wikipedia.org/wiki/Datacoup (last visited April 21, 2020).

[275] *See* Eben, *supra* note 268, at 267–68 (discussing the company People.io and how it purchases personal data with credits); *see also* Kate Cox, *Broadband Industry: It's Unfair If Facebook Can Collect Your Data, But AT&T Can't*, CONSUMER REPORTS (Mar. 29, 2016) https://www.consumerreports.org/consumerist/broadband-industry-its-unfair-if-facebook-can-collect-your-data-but-att-cant/ (citing an AT&T discount offer made to its GigaPower fiber optic customers in 2016).

[276] Elvy, *Paying for Privacy, supra* note 273, at 1391.

[277] *See* Cox, *supra* note 275 (discussing AT&T's discount for personal data offer to its customers).

inflate the costs of their services in order to pay for the discounts being offered. AT&T was accused of exactly this, a "pay for privacy" program where customers unwilling to surrender their privacy were forced to pay more than those who consented.[278] With transparency requirements in place, the same innovative minds that found ways for their business to profit off assets they acquired for free should have no trouble finding ways to reward customers who give consent, without punishing those who do not.

2. Speaking of Transparency . . .

The public sector should not be left out of transparency requirements. People should, at the very least, be made aware when the government is accessing their biometric data and for what purpose. Without this knowledge, we are unable to hold our governments and elected officials accountable with regard to privacy and surveillance, and relying on the goodwill of the FRT users is unacceptable in a society of checks and balances.[279] Situations that require secrecy can be dealt with in much the same way court records and proceedings are sealed depending on the circumstances.[280] Furthermore, keeping the public in the dark about how their biometric data is being used denies the opportunity for a frank and realistic discussion on how the evolution of technology impacts our society and what types of controls we want as a nation and as a global citizen.

In 2013, National Security Agency ("NSA") contractor Edward Snowden revealed to the world that the NSA's PRISM program was monitoring the phone records and Internet activity of millions of Americans and non-Americans with the help of Internet moguls like Google, Apple, and Facebook.[281] The revelations opened a debate on the ethical implications of secret surveillance in the name of national security, and what protections we as a country believed people were entitled to.[282] Each time we learn that our biometric data is being gathered, analyzed, disclosed, and shared without our

---

[278] *Id.*

[279] HAMPSON & JARDINE, *supra* note 151, at 16–17.

[280] *See* Robert Timothy Reagan, *Sealing Court Records and Proceedings: A Pocket Guide*, FEDERAL JUDICIAL CENTER 1–2 (2010), https://www.fjc.gov/content/sealing-court-records-and-proceedings-pocket-guide-0 (explaining generally how and why some court records and proceedings are sealed from the public).

[281] Michael L. Rustad & Thomas H. Koenig, *Towards A Global Data Privacy Standard*, 71 FLA. L. REV. 365, 401 (2019); *Edward Snowden was NSA Prism leak source – Guardian*, BBC NEWS (June 10, 2013), https://www.bbc.com/news/world-us-canada-22836378.

[282] *See The State of Privacy in Post-Snowden America*, PEW RESEARCH CENTER (Sept. 21, 2016), https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/. (discussing the ethics and security debates that occurred in the wake of Snowden's leak of the PRISM program).

knowledge, similar discussions ensue, and public trust in the government and private sector is eroded.[283] It is time this information be publicly reported, and several advantages will flow from such a requirement.

First, this knowledge would protect an individual's Fourth Amendment privacy rights more generally than a provision requiring something as specific as a warrant prior to surveillance. For example, if law enforcement is required to report that it is using FRT to track or identify an individual, agents will be more likely to seek out warrants beforehand, as well as provide this information to a defendant, as a means to prevent both key evidence from later being suppressed in court and convictions from being reversed.[284] Detailed reporting would also shed light on whether the technology was used in approved ways, potentially eliminating highly questionable practices such as using forensic sketches or celebrity photos to identify suspects, which would be cause for a mistrial if something similar were done with fingerprints.[285] Moreover, requiring organizations to divulge when and how they are using FRT—potentially encroaching on First Amendment freedoms as well—will allow government agencies and legislators to model their own reporting framework, one that can withstand public scrutiny and rebuild the public's trust in the government and the commercial industry.[286] These are important wins for rights advocates as well as for the government.

Yet another way to protect individuals with reporting is by monitoring accuracy rates and ensuring they comply with federal requirements. With FRT, better accuracy means less racially biased results.[287] In addition to this oversight, the government could use federal purse strings to incentivize due diligence and compliance with reporting requirements. Congress has the power to regulate most state and local law enforcement FRT systems because

---

[283] *See* HAMPSON & JARDINE, *supra* note 151, at 255 (citing a 2016 CIGI-Ipsos survey where 78 percent of people surveyed were concerned about their information being monitored as a result of the increasing number of Internet enabled devices, and 79 percent expressed concern over the sale and purchase of their private data); *see also* YUE LIU, *supra* note 23 and accompanying text.

[284] *See generally* 1 PRETRIAL MOTIONS IN CRIMINAL PROSECUTIONS § 5-1 (2020) (explaining that suppression of Brady evidence could lead to a reversal of a conviction).

[285] *See Impact Hearing*, *supra* note 20, at 30 (testimony of Clare Garvie); *see also* Harwell, *Police Have Used Celebrity Look-Alikes*, *supra* note 106 (noting questionable uses of FRT such as using altered photos, composite sketches, and celebrity photos to match criminal suspects).

[286] *See* YUE LIU, *supra* note 23 and accompanying text.

[287] *See* Queenie Wong, *Why Facial Recognition's Racial Bias Problem is So Hard to Crack*, CNET (Mar. 27, 2019 5:00 A.M.), https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/ (noting that Amazon improved its FRT accuracy, which "reduced the error rates for identifying women and darker-skinned men by up to 20 times.").

they are purchased with federal funds.[288] Not only could they require certain standards and limits when FRT is used, they could incentivize FRT providers to improve their technology by rewarding better quality with preference in the contract bidding process. With this kind of transparency in place, facial recognition could still be used by government agencies in meaningful ways that are significantly less likely to infringe on individual rights than the current free-for-all in the FRT landscape.

3. It's All About the Money

At the end of the day, all organizations must be profitable. Both private and public sector organizations place high value on financial stability, and threats to profitability are to be avoided at all costs.[289] When it comes to privacy laws, giving people the ability to sue an entity that violates their rights basically empowers them with a weapon all organizations fear: messy, complex, and expensive litigation that is often coupled with negative publicity.[290] Currently, only BIPA and the CCPA grant private individuals this power, and a string of recent high-stakes data breach scandals may prove the private right of action, which could result in actual and statutory damages, is in fact the powerful deterrent it is designed to be.[291]

Under the CCPA, which took effect on January 1, 2020, plaintiffs may seek actual damages or statutory penalties of $100 to $750 per violation.[292] Lawsuits against two major players, home security system company Ring and video conferencing company Zoom, have already been filed by consumers.[293] Meanwhile, under BIPA, statutory penalties alone range from $1,000 to $5,000 *per violation*.[294] In 2019, just one week after Facebook agreed to a

---

[288] *See Impact Hearing*, *supra* note 20, at 14 (testimony of Clare Garvie).

[289] *See Anatomy of Biometric Laws, supra* note 218 (recommending companies take a proactive approach towards compliance with emerging biometric privacy laws because under BIPA, plaintiffs could seek costly statutory damages, injunctive relief, actual damages, and recovery of attorney fees and litigation costs).

[290] *See* Rosenthal & Oberly, *What Companies Can Expect*, *supra* note 170 (contending that BIPA statutory damages are a considerable incentive for plaintiffs and attorneys to pursue class action lawsuits for alleged violations).

[291] *See supra* Section III.B.iii.

[292] *See* Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BAKERLAW 1, 6 (Nov. 21, 2018), https://www.bakerlaw.com/articles/alan-friel-laura-jehl-create-chart-comparing-ccpa-and-gdpr.

[293] *See* Molly F. Martinson, *Zoom and Gloom: Early CCPA Lawsuits Against Zoom Seek to Expand Private Right of Action*, WYRICK PRACTICAL PRIVACY BLOG (Apr. 7, 2020), https://practicalprivacy.wyrick.com/blog/zoom-and-gloom-early-ccpa-lawsuits-against-zoom-seek-to-expand-private-right-of-action (citing the Ring suit filed in February 2020 and two Zoom suits filed in March 2020).

[294] *See* Grande & Kochman, *supra* note 175.

$550 million settlement,[295] a class action suit was filed against Google in Illinois, alleging the tech giant was gathering facial images, converting them to faceprints, and creating face templates without the consumer's consent, in violation of BIPA.[296] The lawsuit adds to a growing list of BIPA suits against major companies, such as The Home Depot and Walmart, and more class actions are likely to be filed unless companies take measures to bring themselves into compliance.[297]

Elsewhere, biometric privacy law protections vary from state to state. Were the federal government to enact a biometric data law allowing for a private right of action, albeit limited, FRT providers and users would have one set of national standards to meet and thus a clear view on how to avoid being sued by private consumers so they can focus on innovation.[298] With the prevalence of FRT being used across state lines and no national guidelines for companies to follow, many predict a surge in litigation that will tie up the courts and cost companies billions in settlements, with no end to this trend in sight.[299] Thus, the incorporation of a private right of action in federal legislation would serve to guide FRT providers and users towards compliance with the regulations.

VI. CONCLUSION

The facial recognition technology used today in everything from home appliances to smartphones to security cameras is thanks to the pace with which creators have been able to develop and improve the technology.[300] While this ability to innovate is laudable, it has been made possible in part thanks to a lack of uniform, federal regulations that would address important

---

[295] *See supra* note 173. (Although the original settlement amount was a record-breaking $550 million, the district judge refused to approve it, citing concerns it would fail to compensate millions of Illinois users. Facebook raised its offer to $650 million in July 2020).

[296] Wendy Davis, *Google Hit With New Lawsuit Over Faceprints*, MEDIAPOST (Feb. 7, 2020), https://www.mediapost.com/publications/article/346807/google-hit-with-new-lawsuit-over-faceprints.html.

[297] *Id.*

[298] *See* Llaneza, *supra* note 140, at 22 (asserting that a federal law granting consumers a private right of action would put companies on notice as to their existing data privacy policies); *see also supra* note 235.

[299] *See* Wong, *supra* note 152, at 252 (expecting litigation to increase under BIPA after recent rulings); *see also* Rosenthal & Oberly, *What Companies Can Expect*, *supra* note 170 (stating that recent court rulings have opened room for extremely costly litigation considering the nature and extent of the violation).

[300] *See* Trepp, *supra* note 15 (noting how FRT has improved dramatically with the assistance of AI).

public concerns, including the infringement of constitutional rights.[301] Despite limited support for the continuation of this "wild west" of biometrics, as well as for some kind of moratorium on FRT use, only a balanced approach will succeed.[302]

The federal government should look to BIPA, the CCPA/CPRA, and the GDPR as guideposts for the implementation of a much needed national standard on FRT, where providers and users, who are the ones benefiting from and profiting off of our data, are the ones to primarily shoulder the burden of FRT's consequences.[303] Congress should pass a law that requires consumers be compensated for their data, that there be detailed reporting on the use of FRT, and that individuals have a private right of action against FRT users.[304] Only when public and private sector organizations are forced to recognize the tangible and protectible value of biometric data will they reckon the impact of FRT on rights we hold to be fundamental.

---

[301] *Supra* Section V.B.
[302] *Id.*
[303] *Supra* Section II.A.ii and II.B.
[304] *Supra* Section V.C.