ARTICLE

NOW YOU SEE ME. NOW YOU STILL DO: FACIAL RECOGNITION TECHNOLOGY AND THE GROWING LACK OF PRIVACY.

SHARON NAKAR & DOV GREENBAUM[1]

Contents

ABSTRACT 889
INTRODUCTION 90
BASICS OF FACIAL RECOGNITION TECHNOLOGY (FRT) 94
THE MANY AND BROAD USES OF FRT 97
UNIVERSAL CONCERNS WITH FRT 100
PRIVACY CONCERNS WITHIN THE US JUSTICE SYSTEM 102
FRT CONCERNS OUTSIDE OF THE US JUSTICE SYSTEM 106
EUROPEAN LEGAL FRAMEWORK 108
PRIVACY CONCERNS RAISED BY CURRENT AND FUTURE USES OF FRT 109
FRT AND THE RIGHT TO BE FORGOTTEN 111
FRT AND THE RIGHT TO ANONYMITY 115
ANTI-MASK LAWS AND FRT 117
OTHER ETHICAL AND LEGAL CONCERNS ASSOCIATED WITH FRT 120
THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION)NTIA(BEST PRACTICES 121
CONCLUSIONS 123

[1] Corresponding Author: Dov Greenbaum, JD, PhD is an Associate Professor of Molecular Biophysics and Biochemistry (adj) at Yale University in New Haven, CT USA. Email: dov.greenbaum@yale.edu. Dov is the Founder and Director of the Zvi Meitar Institute for Legal Implications of Emerging Technologies, Radzyner Law School, Interdisciplinary Center Herzliya, Israel. Sharon Nakar is a Fellow at the Zvi Meitar Institute for Legal Implications of Emerging Technologies, Radzyner Law School, Interdisciplinary Center Herzliya, Israel.
The authors would like to thank the Zvi Meitar Family for their continued support of all of our research endeavors. The authors would also like to thank Liana G. for her help in the editing process. Finally, the authors would like to especially thank Inbar Carmel for her incredible management of the Zvi Meitar Institute.

ABSTRACT

Facial recognition technology allows the government to track the movement of their citizenry in an unprecedented fashion, but at the same time it allows Facebook to find your friends in your most recently uploaded pictures. It is not clear which is the more insidious threat. Whereas European governments have provided some protections for the type of data collected through facial recognition, most recently in the right-to-be forgotten, US courts seem at best split as to whether there is even a right to anonymity that would protect people from being tracked. But even if it exists, this right applies only in relation to state actors and the most recent attempt at developing best practices for private actors arguably failed. New efforts are needed to develop a consensus among all stakeholders before this technology becomes even more entrenched.

INTRODUCTION

The New York State Department of Motor Vehicles (the New York "DMV") recently announced that they will be implementing an enhanced facial recognition system to combat identity theft and fraud. The DMV system will incorporate 8000 new photos each day, adding to an already hefty 16 million photos in its current database.[2] This announcement followed on the heels of an earlier disclosure that New York and New Jersey's DMVs employed facial recognition technology (FRT) in a collaborative effort to arrest three commercial drivers for identification fraud.[3]

There are many consumer advocates that argue that government agencies need to be especially careful when implementing FRT.[4] Like any other form of biometric data —defined for example by the FBI as "measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual"[5] — and other identifying technologies,[6] FRT adds a whole new dimension to the potential violations of privacy and other rights, among a plethora of other legal issues. Most distressingly, biometrics in general, and our faces in particular, are relatively immutable, i.e., they, unlike government or bank issued identification numbers, are hard to change once our identities have been compromised, or our data is unfairly/unknowingly entered into a system.

The Illinois Biometric Information Privacy Act (BIPA)[7] is one of a growing number of state efforts to create statutory limitations as to the use and application of biometric information for both state and non-state actors,[8] likely reflecting a broadly-felt growing concern.[9] Notably, this concern was recently made explicit

[2] *Governor Cuomo Announces Major Enhancement to Department of Motor Vehicles' Facial Recognition Program*, N.Y. STATE (Feb. 22, 2016), https://www.governor.ny.gov/news/governor-cuomo-announces-major-enhancement-department-motor-vehicles-facial-recognition-program [https://perma.cc/NE77-H364].

[3] Joe Morrissey, Casey McNulty & Mairin Bellack, *Press Release – 08-17-2015*, N.Y. STATE DMV (Aug. 17, 2015), https://dmv.ny.gov/press-release/press-release-08-17-2015 [https://perma.cc/6J34-V2KB].

[4] *See, e.g.,* Letter from 18 Million Rising, Advocacy for Principled Action in Gov't, Am.-Arab Anti-Discrimination Comm., and Am. Civil Liberties Union to Erika Brown Lee, Privacy Analyst, U.S. Dep't of Justice (May 27, 2016).

[5] *Fingerprints and Other Biometrics*, FBI, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics (last visited Nov. 10, 2016) [https://perma.cc/5PDK-NG89] ("Fingerprints are a common biometric modality, but others include things like DNA, irises, voice patterns, palmprints, and facial patterns.").

[6] BIOMETRIC SYSTEMS 4 (James Wayman, Anil Jain, DavideMaltoni and Dario Maio eds., 2005) (ebook).

[7] Biometric Information Privacy Act, 740 ILL. COMP. STAT. §14/1 (2008).

[8] *See e.g.*, TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009).

[9] Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/5 (West 2010),

by the President's Council of Advisors on Science and Technology:

> It is foreseeable, perhaps inevitable, that these capabilities will be present in every cell phone and security surveillance camera, or every wearable computer device. (Imagine the process of negotiating the price for a car, or negotiating an international trade agreement, when every participant's Google Glass (or security camera or TV camera) is able to monitor and interpret the autonomic physiological state of every other participant, in real time.) It is unforeseeable what other unexpected information also lies in signals from the same sensors. Once they enter the digital world, born-analog data can be fused and mined along with born-digital data. For example, facial-recognition algorithms, which might be error-prone in isolation, may yield nearly perfect identity tracking when they can be combined with born-digital data from cell phones (including unintended emanations), point-of-sale transactions, RFID tags, and so forth; and also with other born-analog data such as vehicle tracking (e.g., from overhead drones) and automated license-plate reading.[10]

Consumer advocates in favor of reigning in the use of FRT might be facing an easier battle if they were only dealing with concerns resulting from the implementation of FRT by state agencies or even large corporations. However, FRT has gone mainstream: Apple recently announced the incorporation of facial recognition technology into their upcoming iPhone updates,[11] giving the power of facial recognition to tweens.[12] This upgrade to Photos, i.e., what Apple has termed, Advanced Computer Vision, will allow users to catalog their stored images using faces extracted from the images themselves.[13] Notably, Apple isn't

("(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings. [. . .] (d) An overwhelming majority of members of the public are weary of the use of biometrics . . . . (e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions. (f) The full ramifications of biometric technology are not fully known. (g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.")

[10] PRESIDENT'S COUNSEL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 23 (May 2014), http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/LQ8D-97V2].

[11] Brian Barrett, *IOS 10: Every New Feature Coming to Your Iphone*, WIRED (June 13, 2016), http://www.wired.com/2016/06/ios-10-features/ [https://perma.cc/XUL7-JW8J].

[12] Todd Hixon, *What Kind of Person Prefers an iPhone?*, FORBES (April 10, 2014), http://www.forbes.com/sites/toddhixon/2014/04/10/what-kind-of-person-prefers-an-iphone/#5316ac0b3e5a [https://perma.cc/NZ4W-5S9Z].

[13] Kwame Opam, *Apple takes on Google Photos with new Photos update*, THE VERGE

the first platform to provide facial recognition capabilities to the masses. Google[14] and Facebook[15] both offer similar, albeit more cloud-focused, capabilities.

Granted, Apple is taking a substantial legal risk as there are a handful of consumer-facing statutes that have attempted, (although some have failed)[16] to limit the use of FRT. Specifically, the platforms mentioned above, and others, including Facebook,[17] Shutterfly,[18] Snapchat,[19] and Google[20] have each been sued over their implementation of FRT,[21] particularly in Illinois under the BIPA.[22] Notably, BIPA has teeth: as per Section 15: "No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." Further, it provides a private right of action that allows for recovery of $1000 for every negligent violation and $5000 for each intentional violation.[23]

There is no doubt that FRT poses many privacy challenges, particularly when implemented in public places where, if used successfully, it will remove any possibility of anyone's ability to go about their daily business privately and anonymously. As such, it is somewhat disheartening that in light of the recent litigation involving BIPA, that some lawmakers (perhaps somewhat suspiciously, given the timing)[24] were considering substantially weakening BIPA by

(June 13, 2016), http://www.theverge.com/2016/6/13/11922626/apple-photos-update-announced-new-features-wwdc-2016 [https://perma.cc/M9GJ-H7H3].

[14] *Find People, Things, & Places in Your Photos*, GOOGLE, https://support.google.com/photos/answer/6128838 (last visited November 10, 2016) [https://perma.cc/F5C7-H4QZ].

[15] *How does Facebook Suggest Tags?*, FACEBOOK.COM, https://www.facebook.com/help/122175507864081 (last visited November 10, 2016) [https://perma.cc/X9A9-LD6J].

[16] H.R. 1094, 64 Leg., 2015 Reg. Sess. (Wash. 2015).

[17] Gullen v. Facebook.com, Inc., No. 15 C 7681, 2016 WL 245910 at *1-3, (N.D. Ill. Jan. 21, 2016); In re Facebook Biometric Info. Privacy Litig., No. 15-CV-03747-JD, 2016 WL 2593853 (N.D. Cal. May 5, 2016); Complaint at 1, Patel v. Facebook, No. 1:15-cv-04265 (N.D. Ill. May 14, 2015).

[18] Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103 (N.D. Ill. 2015).

[19] Martinez v. Snapchat, Inc., 2016 WL 3000331 (Cal. Super. filed May 23, 2016).

[20] Complaint at 1, Rivera v. Google, Inc., No. 16-02714 (N.D. Ill. filed Mar. 1, 2016).

[21] Christopher Zara, *Google Gets Sued Over Face Recognition, Joining Facebook And Shutterfly In Battle Over Biometric Privacy In Illinois*, INT'L BUS. TIMES, (Mar. 4, 2016, 9:45 AM), http://www.ibtimes.com/google-gets-sued-over-face-recognition-joining-facebook-shutterfly-battle-over-2330278 [https://perma.cc/V3WN-8QR4].

[22] 740 ILL. COMP. STAT 14/10 (2008).

[23] 740 ILL. COMP. STAT. 14/20 (2008).

[24] Jeff John Roberts, *Tech Giants Allegedly Behind 11th Hour Push to Gut Face Recognition Law*, FORTUNE, (May 27, 2016, 3:39 PM), http://fortune.com/2016/05/27/biometrics-

limiting enforcement to only instances where the offending concerns involve "data resulting from an in-person process whereby a part of the body is traversed by a detector or an electronic beam." (E.g., not your library of photographs on your phone.)[25]

Fortunately, that particular amendment has been shelved indefinitely, but in other jurisdictions as well, efforts to protect privacy from the growth of FRT are also coming up short. Consumer advocates[26] in conjunction with the National Telecommunications and Information Administration (NTIA)[27] have finally released a set of facial recognition technology best practices for commercial (but explicitly not government) implementation.[28] It is weak, and unsupported by a number of stakeholders. Moreover, the guidelines were initially supposed to be part of a now tabled Federal Privacy law. Without that federal law in place, the guidelines remain simply unenforceable suggestions.[29]

Despite all of the concerns and challenges, facial recognition systems will continue to become more pervasive and common. Not only will governments and corporations continue to incorperate FRT into varied aspects of their management software tools, but as Apple, Google and others have shown, there is a strong consumer demand for access to this technology as well.

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.[30]

---

law/ [https://perma.cc/WWX3-BWWG].

[25] H.R. 6074, 99th Gen. Assemb., Reg. Sess. (Ill. 2016).

[26] E.g., Alvaro Bedoya, Center for Digital Democracy, Common Sense Kids Action, Consumer Action, Consumer Federation of America, Consumer Watchdog, Privacy Rights Clearinghouse, and U.S. PIRG, Center for Democracy and Technology, Consumer Technology Association, Interactive Advertising Bureau, NetChoice, Software & Information Industry Association and the International Biometrics Industry Association.

[27] Privacy Multistakeholder Process: Facial Recognition Technology (June 17, 2016), NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION, https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology [https://perma.cc/DB5T-LWN4].

[28] NAT'L TELECOMM. & INFO. ADMIN., PRIVACY BEST PRACTICE RECOMMENDATIONS FOR COMMERCIAL FACIAL RECOGNITION USE (2016).

[29] Justin Brookman, *CDT Withdraws from the NTIA Facial Recognition Process*, CTR. FOR DEMOCRACY & TECH. (June 16 2015), https://cdt.org/blog/cdt-withdraws-from-the-ntia-facial-recognition-process/ [https://perma.cc/MY3R-CHWH].

[30] Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 434-35 (2013).

However, it is not all bad, FRT also has the potential to promote innovation in many different sectors. Businesses may use this technology to lower security expenses or to improve services for consumers, by fulfilling a very real need for reliable identification and authentication online and offline.[31]

In this paper we provide a basic introduction to the very complex technologies associated with facial recognition. We describe the general uses of the technology, both as a police tools as well as an emerging consumer tool, and the general fears associated with the increasing usage of the technology, particularly the privacy concerns. We provide some analysis of the legal frameworks that can and have been used to limit the use of this technology.

Moving from legal frameworks we look to emerging legal theories associated with the right to be forgotten and the right to anonymity and anti-mask laws to ascertain whether these theories can be applied to allay the privacy fears associated with FRT.

Finally, we review the most recent (failed) efforts to create a set of best practices to be applied to the use of FRT and draw some conclusions and suggestions for the future.

BASICS OF FACIAL RECOGNITION TECHNOLOGY (FRT)

Facial Recognition Technology is used primarily for the identification of individuals. It is one of several biometric authentication technologies such as fingerprinting, palm veins analysis, DNA sequencing, palm printing, and iris recognition.

In the 1960s, scientists (both civilian and military) began to explore the technological ability to "identify, at a distance, specific individuals among the enemy ranks".[32] In the 1970's researchers from Stanford University in California and Kyoto University in Japan began to develop the ability to identify facial forms in face forms out of images.[33] Eventually the technology evolved to the current state of the art.[34] Generally the facial recognition systems are designed today to seek out patterns in captured images that compare favorably to facial model. Systems are typically programmed such that when a pattern is found to resemble

[31] *E.g.*, *Human Interface & Biometric Devices - Emerging Ecosystems*, JUNIPER RESEARCH, http://www.juniperresearch.com/researchstore/enabling-technologies/human-interface-biometric-devices/emerging-ecosystems-opportunities [https://perma.cc/RY6C-YGCP] (last visited Nov. 11, 2016).

[32] KELLY A. GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE 29 (2011) (ebook).

[33] *Id*. at 29-31.

[34] *See* U.S. GOV'T. ACCOUNTABILITY OFF., GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 3-4 (2015) [hereinafter GOV'T ACCOUNTABILITY OFFICE, USES, ISSUES, AND LAW], http://www.gao.gov/assets/680/671764.pdf.

a facial model, the software generates the assumption that there is a face presented in the photo.

In general, biometric technologies identify people by features that distinct to each individual and cannot be changed easily.

Most modern FRT, like other biometric efforts, consists of two processes, enrollment and matching. In FRT these two processes can be further broken down into four main components:[35]

1. Capture: the image, such as through a camera, or purchasing the image from a database of images, for example, from the department of motor vehicles.

2. Deconstruction: creating a digital and searchable representation of the face via complex algorithms which, among other things, divide the face into nodal points, that should not change much with age, such as eye sockets or nose shape. In addition to this geometric approach wherein the system determines the surrounding location and the spatial relationship between the nodal points, other algorithms may use similar efforts to deconstruct the face, for example: (i) Skin texture analysis wherein the system maps a person's unique placement of lines, spot and pores in his skin.; (ii) Photometric approach wherein the algorithmic interpretation of a face is effectively a weighted combination of standardized faces;

3. Store housing: intelligently storing the deconstructed digital representation, and in some cases the original, in vast searchable databases. In some systems, following the initial analysis, the system applies a standardization process to the photo and saves the photo, as well as all other photos in the database using a consistent format. This saved photo becomes the foundation for the eventual faceprint by extracting facial features from the photo.

4. Comparison: employing algorithms to compare a captured image and/or it digital representation to the images collected and stored in the database.

Facial recognition technologies, which are typically evaluated based on their false positive and true positive rates, have a variety of practical and often nonnefarious applications, including: verification, by using a facial recognition algorithm the system can compare between two faceprints[36] and produce a scored value representing the similarity between the two faces; identification, a process where the system can mathematically compare a photo to some or all of the files within a database; and, facial classification, wherein the system can classify each faceprint into numerous categories, such as gender and age.

Facial recognition algorithms are a work in progress and they remain far from

---

[35] *See generally*, Wenyi Zhao et al., *Face recognition: A literature survey*. 35 ACM COMPUTING SURVEYS (CSUR) 399 (2003).

[36] U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY (2016), http://www.gao.gov/assets/680/677098.pdf [https://perma.cc/ZA46-B3CG] [hereinafter GOV'T ACCOUNTABILITY OFFICE, PRIVACY AND ACCURACY].

perfect. The accuracy of systems (e.g., said "false positive and true positive rates") are affected and hampered by the environment, aging, different emotions and dissimilarities between the compared images, such as the images lighting conditions, camera distance, background, head orientation and size of the face in the image. (Collectively known as a-pie: aging, posing, illumination and emotion.)[37] More specifically, it was found that the identification performance drops dramatically when outdoor images are used in contrast to indoor images. Further, with the bulk of the images in police databases being collected from surveillance cameras many systems suffer from poor image quality. Additionally, the time delay between the collection and analysis of the database image and the probe image can introduce substantial error, even after only a year.[38] Finally, the size of the database can overwhelm some of the more simpler facial recognition algorithms.[39] However, as the technology develops, facial recognition systems will be even more effective.

Senator Al Franken, chairman of the US Senate Judiciary Subcommittee on Privacy, Technology, and the Law, said he has "serious concerns about facial recognition technology and how it might shape the future of privacy."[40] In an open letter to the founder of NameTag app,[41] a commercially available facial recognition app that lets users match a face to their online and public record, Senator Franken differentiated FRT from other biometric technology:

> Unlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a distance, without the knowledge or consent of the person being identified. Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere-on a lamppost across the street, attached to an unmanned aerial vehicle, or, now, integrated into the eyewear of a stranger.[42]

What are the uses that Senator Franken is afraid of?

---

[37] MOSTAFA A. FARAG, FACE RECOGNITION IN THE WILD (Dec. 2013), http://ir.library.louisville.edu/cgi/viewcontent.cgi?article=3352&context=etd [https://perma.cc/AD9D-VE7E].

[38] U.S. GOV'T ACCOUNTABILITY OFF., GAO-03-174 TECHNOLOGY ASSESSMENT: USING BIOMETRICS FOR BORDER SECURITY (2002), http://www.gao.gov/assets/160/157313.pdf [https://perma.cc/T9PL-KBBY].

[39] *Id.* at 57.

[40] *Sen. Franken Raises Concerns about Facial Recognition App that Lets Strangers Secretly Identify People*, AL FRANKEN | SENATOR FOR MINNESOTA (Feb. 5, 2014), http://www.franken.senate.gov/?p=press_release&id=2699 [https://perma.cc/5KAW-NJTN] [hereinafter *Franken*].

[41] *NameTag on the App Store*, APPLE (Apr. 9, 2015), https://itunes.apple.com/us/app/nametag/id690843187 [https://perma.cc/4XWQ-DTSH].

[42] *Franken*, *supra* note 40.

THE MANY AND BROAD USES OF FRT

Notwithstanding its current limitations, FRT is already implemented in many areas such as security, commerce, social media,[43] personal use, and even for religious purposes.[44] The breadth of its uses reveals the depth of its engagement in our lives.

For example, in recent years many police departments have adopted facial recognition software to pursue prostitutes, drug dealers and other non-violent suspects.[45] Notably FRT is far from the first foray of the police into biometrics; fingerprinting has been around for decades,[46] as has been the use of genetic markers by national police forces such as the FBI's CODIS (Combined DNA Index system) database.[47] Notably though, facial recognition software has been shown to be much faster in helping to identify suspects than many alternatives.[48] Its growing prevalence in police work notwithstanding, there remain many concerns about the potential misuse of the technology. These concerns are exacerbated by the lack of guidelines and oversight and the ability to easily populate the databases.

But even with big databases, the police have failed to prove FRT's current effectiveness: San Diego county documents from 2011, show that only a quarter of the 20,600 uses of facial recognition resulted in a match to a criminal record.[49] Given these low hit rates many might question their broad use given the associated concerns. Some fundamental principles that might be incorporated in police standard operating procedures of facial recognition might include technically

[43] U.S. Patent Application Serial No. 13/779,497, Publication No. 0280682 (published Oct. 24, 2013) (Innerscope Research, Inc., applicant); Man Qi & Denis Edgar-Nevill, *Social networking searching and privacy issues*, *in* 16 INFORMATION SECURITY TECHNICAL REPORT 74, 76 (2011).

[44] *See, e.g.*, Ben Buckley & Matt Hunter, *Say cheese! Privacy and facial recognition,* 27 COMP. L. & SECURITY R. 637 (2011) (enumerating the wide ranging applications of FRT).

[45] Timothy Williams, *Facial Recognition Software Moves From Overseas Wars to Local Police,* N.Y. TIMES (Aug. 12, 2015) http://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html [https://perma.cc/7WVU-JJQB].

[46] SIMON A. COLE, SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION 1 (2001).

[47] Bruce Budowle et al, *CODIS and PCR-Based Short Tandem Repeat Loci: Law Enforcement Tools*, *in* SECOND EUROPEAN SYMPOSIUM ON HUMAN IDENTIFICATION (1998); Dov Greenbaum, & Sharon Nakar, *Editorial Thematic Issue: Genomics and Criminal Law*, *in* 8 RECENT ADVANCES IN DNA & GENE SEQUENCES 57 (2014).

[48] Timothy Williams, *Facial Recognition Software Moves From Overseas Wars to Local Police*, N.Y. TIMES (Aug. 12, 2015), http://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html [https://perma.cc/E6NG-FQHQ].

[49] *Id.*

improving and testing the system before it is broadly implement. Further, perhaps like other police databases that contain substantial amounts of personal and private information, like the Justice For All Act of 2004 that limited access to the national CODIS database and provided stiff penalties for misuse,[50] officers should not necessarily have an unlimited right to every person's data, without showing some special need.

Or alternatively, the recent failings of the state of the art FRT in searching for the Boston Marathon Bombing suspects[51] suggest that research in FRT implementation is not being executed fast enough to effect good police work,[52] prompting more investment and further breaches of privacy rather than limiting simply limiting the use of the technology. A 2013 study supports the former conclusion. In that study, researchers simulated a possible identification scenario using low quality face images of uncooperative subjects and a commercial face matcher returned a rank-one hit for Boston Marathon Bombing suspect Dzhokhar Tsarnaev against a one million mugshot background database.[53]

Police efforts also suggest that we are moving toward more efforts to improve the technology rather than surrendering to the idea that the technology may not yet be sufficiently supplicated and should be shelved until such time. How so? National police programs are also working toward broader implementation of FRT. The US Federal Bureau of Investigation (FBI) has its own identification program. The program will collect several types of data such as iris scans, fingerprints, and photos and match images such as driver's license photos with stills from surveillance cameras. Amy Hess, Executive Assistant Director, Science and Technology Branch; Federal Bureau of Investigation, clarified the program uses: "While the Next Generation Identification technology could theoretically be used to search a wide range of photos, in practice it searches only against a pool of existing mug shots. The database is not a repository for Department of

[50] U.S. DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, FS 000311, OVC FACT SHEET: THE JUSTICE FOR ALL ACT (2016), http://ojp.gov/ovc/publications/factshts/justforall/fs000311.pdf [https://perma.cc/NVA7-ZJ3M].

[51] Sean Gallagher, *Why Facial Recognition Tech Failed in the Boston Bombing Manhunt*, ARS TECHNICA, (May 7, 2013), http://arstechnica.com/information-technology/2013/05/why-facial-recognition-tech-failed-in-the-boston-bombing-manhunt/ [https://perma.cc/8G9Z-X7K9].

[52] JOSHUA C. KLONTZ & ANIL K. JAIN, A CASE STUDY ON UNCONSTRAINED FACIAL RECOGNITION USING THE BOSTON MARATHON BOMBINGS SUSPECTS 2-4 (2013), http://se-nec-com-org.onenec.net/en_SE/en/global/solutions/safety/pdf/MSU_Case_Study_on_Face_Recognition.pdf [https://perma.cc/FK4H-CQVJ].

[53] *Id.*

Motor Vehicle photographs or surveillance photos."[54] Hess' clarification highlights some appreciation of the public's fear of a more pervasive Big Brother. Part of this identification program is the Next Generation Identification-Interstate Photo System (NGI-IPS) which, like other biometric services provided by the FBI, can be modulated as per the needs of the agency using the service.[55] Currently the service, ostensibly implemented under statutory authority,[56] employs an automated process that returns lists of 2 to 50 candidate photographs from a database of 30 million in response to queries from law enforcement. Within the FBI itself, an aptly unit, the Facial Analysis, Comparison and Evaluation (FACE), employs NGI-IPS and similar facial recognition technologies in ongoing investigations.[57]

Like continued efforts by the police to improve FRT, corporations are also seeking to expand the usefulness of the technology. Soon, if not already, simply by walking past a store putative customers might be identified by camera, and be alerted about sales in the vicinity.[58] From a marketing perspective, having information about nearby customers is an invaluable sales opportunity that can drive additional customer engagement. This new feature may also deal with bringing costumers to shop in-store instead of using e-commerce by offering special and timely "deals at the door." Facial-recognition software, like the more inelegant customer loyalty cards, can also help marketers learn valuable information about shoppers profiles over time, for example trends, shopping timing and more.

This isn't far-fetched technology from sci-fi films like personalized advertising in the Tom Cruise blockbuster *Minority Report*.[59] There are already billboards that engage with passing costumers by using simplistic facial-recognition software that can identify the costumer gender, age, and even their mood. By this information gathering the billboard can offer a real time personalized advertising.[60] Further, Kraft foods is developing a similar technology to be used in

---

[54] Amy Hess, Letter to the Editor, *How the F.B.I. Uses Facial Recognition Analysis,* N.Y. TIMES (Aug. 14, 2015), http://www.nytimes.com/2015/08/15/opinion/how-the-fbi-uses-facial-recognition-analysis.html [https://perma.cc/6MPE-TFUY].

[55] *FBI Announces Full Operational Capability of the Next Generation Identification System*, FED. BUREAU OF INVESTIGATION (Sept. 15, 2014), https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system [https://perma.cc/Z8UQ-ZFEH].

[56] 28 U.S.C. § 534 (2012).

[57] GOV'T ACCOUNTABILITY OFFICE, PRIVACY AND ACCURACY, *supra* note 36.

[58] Jason Warnock, *How Facial-Recognition Software Will Shape The Future Of Email Marketing*, MARKETING LAND (Dec. 8, 2015), http://marketingland.com/facial-recognition-software-will-shape-future-email-marketing-154713 [https://perma.cc/K9P2-ACSE].

[59] MINORITY REPORT (20th Century Fox 2002).

[60] Heather Fletcher, *Facial Recognition: Ads Target Consumers for You*, TARGET

supermarkets.[61] Stores and casinos also use this technology to prevent previously identified unwanted guests like card counters and shoplifters from entering.[62]

The television ratings industry further envisions the use of FRT and smart TV to measure television audiences.[63] Smart TVs, or those equipped with associated cameras such as the Xbox's Kinnect would recognize who is watching TV, and even how they react to television programming or advertising. This would help marketers more precisely rate their viewing audience as well as gauge their responses to content and advertising. Smart TV's with FRT already exist,[64] and it is a matter of time before marketers will begin to deploy their vision.

Consumers are still nevertheless skeptical: a recent survey found that while 75% of consumers would decide not to shop at a shop that employs FRT, however, 55% would be positive towards the marketing technology use if they themselves would benefit, for example in obtaining personalized discounts.[65]

FRT is obviously not going away. Why should this concern us?

UNIVERSAL CONCERNS WITH FRT

In general, the expansive use of FRT raises several universal ethical concerns. Most prominently, the tension between the technology and the right to privacy highlight the dialectic between national security and law enforcement, economic

MARKETING (Oct. 5, 2015), http://www.targetmarketingmag.com/article/facial-recognition-ads-target-consumers/all/ [https://perma.cc/3G4N-T7E2].

[61] *Compare* Kashmir Hill, *Kraft To Use Facial Recognition Technology To Give You Macaroni Recipes*, FORBES (Sept. 1, 2011), http://www.forbes.com/sites/kashmirhill/2011/09/01/kraft-to-use-facial-recognition-technology-to-give-you-macaroni-recipes/#3e59f86a301c [https://perma.cc/KQR9-TDEW], *with* Clare McDonald, *Almost 30% of retailers use facial recognition technology to track consumers in store,* COMPUTER WEEKLY.COM (Sept. 15, 2015), http://www.computerweekly.com/news/4500253499/Almost-30-of-retailers-use-facial-recognition-technology-to-track-consumers-in-store [https://perma.cc/Y75H-5NEJ], *and* Laura Northrup, *This Freezer Case Knows When You're Frowning At The Bagel Bites*, CONSUMERIST (Jan. 19, 2016), https://consumerist.com/2016/01/19/this-freezer-case-knows-when-youre-frowning-at-the-bagel-bites/ [https://perma.cc/H7C3-MSA9].

[62] Brown, *supra* note 30 at 428.

[63] Steve McClellan, *Nielsen Explores Facial Recognition Tech For Ratings*, MEDIAPOST (January 22, 2013), http://www.mediapost.com/publications/article/191651/nielsen-explores-facial-recognition-tech-for-ratin.html [http://perma.cc/4RTC-5AVT].

[64] *Samsung Global Privacy Policy - SmartTV Supplement*, SAMSUNG (last visited Oct. 23, 2016), http://www.samsung.com/uk/info/privacy-SmartTV.html [http://perma.cc/6RV5-48HP].

[65] *First Insight Finds What Consumers Really Want From Retailers*, THE POINT OF SALE NEWS (Aug. 12, 2015), http://pointofsale.com/PointofSale.com-Blog/First-Insight-Finds-What-Consumers-Really-Want-From-Retailers.html [http://perma.cc/8MFV-4PJG].

efficiency or public health promoted through the application of facial recognition systems, on the one side, and concerns relating to the potential for disproportionately violating fundamental principles on our society such as the right to personal autonomy, anonymity, to be forgotten, to control one's own personal identifying information, and the person right to protect its own human body, on the other.

Additionally, there are some less obvious social justice issues that can arise, as those who can afford plastic surgery procedures to alter a legally problematic profile will do so, allowing the wealthy to escape some of trappings of a FRT.[66]

Most importantly, FRT impinges on our privacy. The right to privacy is a fundamental human right as described in Article 12 of the Universal Declaration of Human Rights.[67] Importantly, it shapes the balance of power between the citizen and the government, between the individual and large business entities and between man and his fellow man. It is a precondition for the democracy development and freedom. Without privacy there is no freedom of speech, freedom of religion or freedom of movement.

In recent years, the right to privacy has been substantially eroded by new technologies that continually threaten it.[68] To some degree this is our own fault. Witness the plethora of banal, and no so banal information that we readily shout out to the world on social media. "The rise of social networking online means that people no longer have an expectation of privacy . . . the privacy was no longer a 'social norm.'"[69] However, to some degree this is not our fault. Granted the new reality of a camera(phone) in every pocket is a consumer failing, but the sprouting of closed circuit cameras on every street corner is the fault of the government and the growing reliance on overly-pervasive surveillance for preventing crime.[70]

---

[66] Richa Singh et al., *Plastic Surgery: A New Dimension to Face Recognition*, 5 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY 441 (2010); Xin Liu, Shiguang Shan & Xilin Chen, *Face Recognition After Plastic Surgery: A Comprehensive Study*, *in* 2 COMPUTER VISION – ACCV 2012 at 565 (2013).

[67] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

[68] Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, The GUARDIAN (Jan. 11, 2010), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy [https://perma.cc/K25A-JRJF].

[69] *Id*.

[70] *See*, *e.g.*, RACHEL ARMITAGE, NACRO, TO CCTV OR NOT TO CCTV? A REVIEW OF CURRENT RESEARCH INTO THE EFFECTIVENESS OF CCTV SYSTEMS IN REDUCING CRIME (2002), https://epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf; Clive Norris, Mike McCahill & David Wood, Editorial, *The Growth of CCTV: a Global Perspective on the International Diffusion of Video Surveillance in Publicly Accessible Space*, 2 SURVEILLANCE & SOCIETY 110 (2004); Barrie Sheldon, *Camera Surveillance within the UK: Enhancing Public Safety or a Social threat?,* 25 INT'L REV. OF L., COMPUTERS & TECH. 193 (2011).

PRIVACY CONCERNS WITHIN THE US JUSTICE SYSTEM

Although the word "privacy" does not specifically appear in the United States Constitution, most legal authorities generally agree that there exists a constitutional right of privacy, stemming from some penumbra of one of the Amendments.[71] For example, some have found a source of privacy rights in either the First,[72] Third, Fourth,[73] or Fifth Amendments. Notably, privacy rights do explicitly exist in some state constitutions, like that of California.[74]

Academically, most privacy jurisprudence in the area of tort law in the United

[71] Griswold v. Connecticut, 381 U.S. 479, 483 (1965).

[72] NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958).

[73] Katz v. United States, 389 U.S. 347, 352-353 (1967); Olmstead v. United States, 277 U.S. 438, 471 (1928) (Brandeis, J. Dissenting).

[74] CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy"); See, also, ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed"); ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law"); FLA. CONST. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein"); HAW. CONST. art. I, § 6 ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest"); ILL. CONST. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means") (emphasis added); LA. CONST. art. 1 § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy") (emphasis added); MONT. CONST. art. 2, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest"); MO. CONST. art 1, § 15 ("That the people shall be secure in their persons, papers, homes, effects, and electronic communications and data, from unreasonable searches and seizures; and no warrant to search any place, or seize any person or thing, or access electronic data or communication, shall issue without describing the place to be searched, or the person or thing to be seized, or the data or communication to be accessed, as nearly as may be; nor without probable cause, supported by written oath or affirmation"); S.C. CONST. art. 1, § 10 ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy 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, the person or thing to be seized, and the information to be obtained") (emphasis added); WASH. CONST., art. 1, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.") *See also Privacy Protections in State Constitutions*, National Conference of State Legislatures (Dec. 3, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx [https://perma.cc/3RXQ-Z25E].

States is typically traced back to the Warren and Brandeis paper from 1890,[75] itself possibly influenced by another paper by Godkin the same year.[76] By the early turn of the century, courts began to apply Warren and Brandeis in the development of privacy torts.[77] In *United States v. Blok* the DC Circuit noted that the right to privacy is "one of the unique values of our civilization False"[78] In addition to broad constitutional protections, many jurisdictions also have numerous statutorily defined rights of privacy that seek to limit access to private and/or personal information. However, the right of privacy should be "balanced against the state's compelling interests[,]" such as "public morality, protection of the individual's psychological health," and other pertinent concerns.[79] Much of our current understanding of privacy also stems from Dean Prosser's article in 1960 where he outlined his four canonical privacy torts.[80]

Privacy law has developed throughout the following decades — the US Congress has passed a number of laws protecting individual privacy rights[81] — and

[75] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 6 HARV. L. REV. 193 (1890).

[76] E. L. Godkin, *The Rights of the Citizen, IV—To His Own Reputation*, SCRIBNER'S MAGAZINE, July 1890, at 58.

[77] *See* Roberson v. Rochester Folding Box Co., 64 N.E. 442, 443 (N.Y. 1902); Pavesich v. New England Life Ins. Co., 50 S.E. 68, 74 (Ga. 1905).

[78] United States v. Blok, 188 F.2d 1019, 1020 (D.C. Cir. 1951).

[79] *Privacy*, CORNELL U. L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/privacy [https://perma.cc/7MZD-LHZH].

[80] *See generally* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

[81] DANIEL J. SOLOVE ET AL., PRIVACY, INFORMATION, AND TECHNOLOGY 31 (2006) (Listing the Privacy Act of 1974, 5 U.S.C. § 552a (2012)); Family Educational Rights and Privacy Act of 1974 20 U.S.C. § 1232g (2012); Fair Credit Reporting Act of 1970 15 U.S.C. § 1681 (2012); Right to Financial Privacy Act of 1978 12 U.S.C. §§ 3401-3422 (2012); Video Privacy Protection Act of 1988 18 U.S.C. § 2710 (2012); Computer Matching and Privacy Protection Act of 1988 5 U.S.C. § 552a (2012); Employee Polygraph Protection Act of 1988 22 U.S.C. §§ 2001-2009 (2012); Electronic Communications Privacy Act of 1986 18 U.S.C. §§ 2510-2522 (2012); Cable Communications Policy Act of 1984 47 U.S.C. § 551 (2012); Privacy Protection Act of 1980 42 U.S.C. ch. 21A (2012); Foreign Intelligence Surveillance Act of 1978 50 U.S.C. ch. 36 (2012); Telephone Consumer Protection Act of 1991 47 U.S.C. § 227 (2012); Driver's Privacy Protection Act of 1994 18 U.S.C. § 2721 (2012); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No.104-191, 110 Stat. 1936 (codified as ammended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C. (2012)); Identity Theft and Assumption Deterrence Act of 1998 18 U.S.C. § 1028 (2012); Children's Online Privacy Protection Act of 1998 15 U.S.C. §§ 3501-6506 (2012); Gramm-Leach-Bliley Act of 1999, Pub. L. No.106-102, 113 Stat. 1338 (codified as ammended in scattered sections of 12 U.S.C. (2012)); CAN-SPAM Act of 2003 15 U.S.C. §§ 7701-7713 (2012); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as ammended in scattered sections of 15 U.S.C. (2012)); Video Voyeurism Prevention Act of 2004 18 U.S.C. § 1801 (2012).

often it has had to expand its scope substantially as technology allowed deeper and more commonplace intrusions into privacy.

Perhaps one of the most pertinent cases is *Lidster*. The Supreme Court, in *Illinois v. Lidster*,[82] ruled on issues relating to unwarranted and public surveillance. Here, the legality of setting up a traffic checkpoint in order to identify the suspect in a severe hit and run accident was questioned.[83] Lidster argued that catching the right suspect, is less important than protecting the privacy of the people that were subjected to the police use of surveillance.[84] The court found otherwise: the Fourth Amendment permits the police use of surveillance in these instances.[85] Reflecting on the decision, Judge Posner noted that "*Lidster* is important because it divorces searching from suspicion. It allows surveillance that invades liberty and privacy to be conducted because of the importance of the information sought, even if it is not sought for use in a potential criminal proceeding against the people actually under surveillance."[86]

It is useful to see how the court applies the law to emerging invasive technologies. For example, in *Kyllo v. United States*,[87] the court found that the use a thermal imaging device outside of Danny Lee Kyllo's home, to search for radiating heat assumed to be associated with marijuana cultivation, and to then obtain a search warrant based on that information was an unlawful search. Along with the many opportunities derived by the new FRT, to track, locate and associate criminals, the potential for abuse still exists, and the tension between it and the right to privacy will likely quickly come to the courts.

In a recent summary of the law, the Arizona Court of Appeals noted that:

> Even in the absence of a trespass, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable. However, a search does not occur unless an individual exhibits an expectation of privacy and society is willing to recognize that expectation as reasonable.[88]

In most contexts the use of facial recognition would seem to take place in areas and situations wherein the individual has little to no expectation of privacy.

As such, case law suggests that what we knowingly make public is not protected by the Fourth Amendment that protects citizens from unlawful searches

---

[82] Illinois v. Lidster, 540 U.S. 419, 427-28 (2004).

[83] *Id.* at 422.

[84] *Id.*

[85] *Id.* at 428.

[86] RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 91 (2006).

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

[88] State v. Estrella, 286 P.3d 150,153 (Ariz. Ct. App. 2012) (quoting *Kyllo*, 533 U.S. at 33).

and seizures. For example, in *Katz v. United States*,[89] the plaintiff argued that the government could not "introduce evidence of the petitioner's end of telephone conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls." The court agreed, and noted that it should be "recognized that the Fourth Amendment protects people— and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[90] However, the court did note that: "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[91] This lack of privacy in public was also found to be the case in *California v Ciraolo*: "The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[92]

As an aside, the courts have also struggled with deciding what is and what is not a tracking device, i.e., something that might run afoul of the Fourth Amendment rights.[93] It is unclear whether technology that allows the automated tracking of an individual from one security camera to the next would constitute a tracking device requiring a warrant.[94]

With regard to the use of facial recognition technology in the courts, while there seems to be no specific cases, there has been at least one prophetic example: and repeated in *People v. Johnson*,[95] and repeated in *People v. Xiong*,[96] the California Court of Appeal suggested that in the use of FRT,

> [T]he database search merely provides law enforcement with an investigative tool, not evidence of guilt . . . the means by which a particular person comes to be suspected of a crime—the reason law enforcement's investigation focuses on him—is irrelevant to the issue to be decided at trial, i.e., that person's guilt or innocence, except insofar as it provides independent evidence of guilt or innocence. For example, assume police are investigating a robbery. The victim identifies 'Joey' as the perpetrator. The means by which 'Joey' becomes the focus of the investigation—the eyewitness

[89] Katz v. United States, 389 U.S. 347, 348 (1967).

[90] *Id.* at 353.

[91] *Id.* at 351-52 (citing Lewis v. United States 385 U.S. 206, 210 (1967)).

[92] California v. Ciraolo, 476 U.S. 207, 213 (1986) (allowing for the observation of marijuana plants from the air).

[93] United States v. White, 62 F. Supp. 3d 614, 624 (E.D. Mich. 2014).

[94] *E.g.*, 18 U.S.C. § 3117 (2012).

[95] People v. Johnson, 43 Cal. Rptr. 3d 587, 597-98 (Cal. Ct. App. 2006).

[96] People v. Xiong, 155 Cal. Rptr. 3d. 877, 890 (Cal. Ct. App. 2013).

> identification—is relevant because that identification is itself evidence of guilt. Suppose instead that a surveillance camera captures the robbery on tape. Police use facial recognition software to check the robber's facial features against driver's license photographs. When the computer indicates a match with 'Joey,' officers obtain his name and address from DMV records, then go to his house and interview him. In the course of the interview, 'Joey' confesses. Whether facial recognition software is discerning and accurate enough to select the perpetrator, or whether it declared a match involving many different people who resembled 'Joey,' or how many driver's license photographs were searched by the software, is immaterial: what matters is the subsequent confirmatory investigation. Stated another way, the fact that the perpetrator's features appear to match those of someone in the DMV database does not affect the strength of the evidence against 'Joey'; it is simply a starting point for the investigation[97]

Finally, specifically within the more modern justice system, the FBI is developing advanced technologies for FRT. With regard to the privacy aspects of the FBI's systems, they are likely governed by at least two statutes, including the Privacy Act of 1974[98] and the E-Government Act of 2002.[99] Under these laws,[100] the FBI is obligated to conduct Privacy Impact Assessments (PIA) for their facial recognition programs. In addition, the FBI is required to employ the Fair Information Practices Principles, i.e., "the foundation and guiding principles of the Department's privacy program."[101] These obligations notwithstanding, the General Accountability Office (GAO) recently found that the FBI had substantial room for improvement in many of these areas, in employing their heretofore not rigorously field-tested systems.[102]

FRT Concerns Outside of the US Justice System

Although the FBI may be constrained by statutes in the area of FRT, the US

---

[97] *Johnson*, 43 Cal. Rptr. 3d at 597-98.

[98] The Privacy Act of 1974, 5 U.S.C. § 552 (2012).

[99] The E-Government Act of 2002, 44 U.S.C. § 101 ("The purposes of this subchapter are to . . . ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to (A) privacy and confidentiality, including section 552a of title 5 [Privacy Act of 1974].").

[100] Gov't Accountability Office, Privacy and Accuracy, *supra* note 36, at 2.

[101] *See, e.g.*, U.S. Dep't. of Homeland Security, Memorandum No. 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (2008), https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf.

[102] *See generally* Gov't Accountability Office, Uses, Issues, and Law *supra* note 34, at 38.

Congress had not yet established federal privacy law regulating the commercial uses of FRT, and all the potentially relevant laws currently on the books do not fully address the privacy core issues of FRT. These existing laws typically govern only the use, collection and storage of one's personal data that may eventually be cross-referenced with the commercial use of FRT. Moreover, many of these laws are specific to financial institutions and health care entities.[103] But not all. There is an emerging group of much more relevant privacy laws that will limit corporate actors from misusing FRT.

The two states that have laws that focus on limiting the use of biometrics, including FRT are Texas and Illinois, which has instituted the Illinois Biometric Information Privacy Act. These states generally require that (i) notice and opt out provisions; (ii)limitations on the commercial use of FRT data acquired; (iii) destruction of the data after three years in Illinois and only one year in Texas; (iv) industry standards of care must be employed to protect private data. Other states, including Washington and California have also proposed laws.[104]

However, a handful of states is obviously insufficient to protect the citizenry. Thus, in light of the current dearth of regulatory oversight, several privacy organizations, governments and industries proposed voluntary privacy guidelines for the commercial use of FRT. For example, the International Biometrics & Identification Association released In August 2014 "Privacy Best Practice Recommendations for Commercial Biometric Use."[105]

The main points are:

1. FRT operators should obtain and publish privacy policies. The privacy policy should specify the purposes of the data captured, whether any non-biometric data is also collected that can be used to associate with the biometric data, and how long the data will be maintained.

2. Businesses have to provide notice that they are implementing these technologies.

3. Firms need to have sufficient cybersecurity to protect against any potential malfeasance.

And, firms should provide to the consumer with a mechanism that can provide the consumer with their own data upon request, and have a method for implementing any necessary corrections to the data.

---

[103] GOV'T ACCOUNTABILITY OFFICE, USES, ISSUES, AND LAW, *supra* note 34.

[104] Sam Castic, Shea G. Leitch, Aravind Swaminathan and Antony P. Kim, *Biometrics: A Fingerprint for Privacy Compliance, Part I*, ORRICK TRUST ANCHOR (Mar. 4, 2016), http://blogs.orrick.com/trustanchor/2016/03/04/biometrics-a-fingerprint-for-privacy-compliance-part-i/ [https://perma.cc/HF35-DPAJ].

[105] INT'L BIOMETRICS & IDENTIFICATION ASS'N, IBIA PRIVACY BEST PRACTICE RECOMMENDATIONS FOR COMMERCIAL BIOMETRIC USE (Aug. 2014), https://www.ntia.doc.gov/files/ntia/publications/ibia_privacy_best_practice_recommendations_8_18_14.pdf.

In addition, the US Federal Trade Commission also issued a staff report regarding the security and privacy implications of FRT.[106] Like many of their other efforts in the area of privacy and emerging technology, the commission recommended that companies using FRT design their services with privacy and security in mind; Specifically, by implementing:

1. Privacy by Design: Companies should build in privacy at every stage of product development.

2. Simplified Consumer Choice: For practices that are not consistent with the context of a transaction or a consumer's relationship with a business, companies should provide consumers with choices at a relevant time and context.

3. Transparency: Companies should make information collection and use practices transparent.

And while all of the current best practices proposals have not yet been agreed upon by any consensus in the field, nevertheless, most agree on at least obtaining some form of consent before identifying a person through anonymous images data. However, in light of the general lack of actual and reliable consumer protection, some corporations like Google, are limiting the use of FRT: in June 2013 Google announced they would not approve any facial recognition apps for Google Glass.[107]

EUROPEAN LEGAL FRAMEWORK

Facial recognition is used widely in Europe, often in policing borders.[108]

In the European Union, restrictions that might be associated with collecting FRT related data are also not limited to governments. In general, personal data can be gathered legally only under strict conditions and only for defined legiti-

---

[106] FED, TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf [https://perma.cc/PA24-J87F].

[107] Charles Arthur, *Google 'bans' facial recognition on Google Glass – but developers persist*, THE GUARDIAN (June 3, 2013 8:38 AM), https://www.theguardian.com/technology/2013/jun/03/google-glass-facial-recognition-ban [https://perma.cc/HB9J-7UDS].

[108] *Immigration and Passports*, HEATHROW, http://www.heathrow.com/arrivals/immigration-and-passports (last visited Nov. 11, 2016) [https://perma.cc/HB9J-7UDS] ("E-passport gates – arrivals made easy. Automated e-passport gates offer an alternative to conventional passport checks. Simply scan your e-passport at the barrier. The system runs a face-recognition check against the chip in your passport, then if you're eligible to enter the UK the gate opens automatically – all in a matter of seconds."); Matthias Monroy, *EU Adds Facial Recognition Capabilities to Police Databases*, DIE LINKE (May 11, 2016), http://www.andrej-hunko.de/7-beitrag/3103-eu-adds-facial-recognition-capabilities-to-police-databases [https://perma.cc/S3ES-5UEM].

mate purposes. Furthermore, persons and organizations which collect and manage personal information have explicit legal responsibilities to protect that data from misuse. They are obligated to respect certain rights of the data owners which are guaranteed by EU law.[109] In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU to further bring Europe into the digital age. In December of 2015, the European Parliament, the Council and the Commission reached an agreement on the new data protection rules, establishing a modern and harmonized data protection framework across the EU.[110]

The EU regulation addresses several fundamental issues associated with the rights of the data subject, i.e., the individual whose personal data is being processed. These rights grant individuals more control over their personal data, including: (i) the right to rectification, to erasure and 'to be forgotten'; [111] (ii) the right to consent to the processing of personal data;[112] (iii) easier access to personal data;[113] (iv) the right to object to uses of the data, including to the use of personal data for the purposes of profiling;[114] and (v) the right to data portability from one service provider to another.[115]

With these pervasive laws, facial recognition technologies may be problematic in light of these rights.[116] In Europe, perhaps even more onerous than in the US, facial images may also be considered to be sensitive personal data, as they can be used to infer race and gender.[117] As such, under the Data Protection Directive, there are a number of limitations associated with processing facial recognition data, including, Articles, 7, 10 and 11.[118]

Privacy Concerns Raised by Current and Future Uses of FRT

---

[109] *Protection of Personal Data*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/ [https://perma.cc/5BM3-LJP3] (last visited Nov. 11, 2016) ("Everyone has the right to the protection of personal data.")

[110] Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU); Council Directive 2016/680, 2016 O.J. (L 119) 89 (EU); Council Directive 2016/681, 2016 O.J. (L 119) 132 (EU).

[111] Council Regulation 2016/679, 2016 O.J. (L 119) 65 (EU).

[112] Council Regulation 2016/679, 2016 O.J. (L 119) 32 (EU).

[113] Council Regulation 2016/679, 2016 O.J. (L 119) 39 (EU).

[114] Council Regulation 2016/679, 2016 O.J. (L 119) 60 (EU).

[115] Council Regulation 2016/679, 2016 O.J. (L 119) 68 (EU).

[116] *See generally* Buckley & Hunter, *supra*, note 44.

[117] *See, e.g.*, *Murray v. Express Newspapers & Big Pictures Ltd* [2008] EWCA (Civ) 446 (appeal taken from the High Court of Justice Chancery Division; Weller & Ors v. Associated Newspapers Ltd [2015] EWCA (Civ) 1176 (appeal taken from the Queen's Bench Division).

[118] Buckley & Hunter *supra* note 44, at 639; *see also id.* at 640 ("Do European data protection laws provide the right model to regulate this technology? Arguably, they do. Their principle driven approach, both flexible and technologically neutral, allow the development of new and innovative applications whilst curbing excessive and intrusive uses.").

As FRT becomes widespread it can give individuals or businesses the possibility to identify almost any person who goes out into public places, surreptitiously or otherwise, tracking their movement, location and conduct. This will likely result in numerous private and public databases of information, which may be sold, shared or used in ways that the consumer does not necessarily understand or consent to. These databases will likely be exposed to failures and security breaches, information leaks by careless or corrupt employees, hackers or even foreign intelligence agency break-ins. The potential damage is irreversible,[119] creating a constant fear of information or identity theft.

Although some argue that it is possible to overcome the problem of information leaks or hacks through appropriate security measures, recent sensitive data leaks revealing hundreds of thousands of military, business, politician and public figures documents — suggest nothing is safe.[120]

Even without security concerns, the presence of FRT severely damages the ability of regular people to maintain their anonymity in the public space. Akin to the evolving right to be forgotten, people ought to have the right to remain anonymous. And, the network of cameras necessary to make FRT work will further envelop society in the fear that big brother is always watching.[121]

It is not only closed-circuit security cameras that are collecting our images. As per a recent U.S. GAO report,[122] FRT has been integrated to a growing degree with social networking. Although a decade ago most of the online available photos were of celebrities, nowadays there are ever increasing online sources of identified images of private citizens.[123] By integrating the social network data, where citizens share their personal information connected to their face image, businesses would gain valuable data. The GAO report found that "consumers generally do not have the right to prevent their personal information from being

---

[119] Andy Adler, *Biometric System Security*, *in* HANDBOOK OF BIOMETRICS 381 (Patrick Flynn, Anil K. Jain & Arun A. Ross eds., 2008).

[120] Luke Harding, *What Are the Panama Papers? A Guide to History's Biggest Data Leak*, THE GUARDIAN (Apr. 5, 2016, 05:42 EDT), http://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers [https://perma.cc/C49N-YZYR].

[121] *See generally* GOV'T ACCOUNTABILITY OFFICE, PRIVACY AND ACCURACY, *supra* note 36.

[122] *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE (2013), http://www.gao.gov/assets/660/658151.pdf [https://perma.cc/9TLG-VU2B].

[123] Alessandro Acquisti, et al., Professors, Carnegie Mellon University, *Faces of Facebook: Privacy in the Age of Augmented Reality, Presentation at BlackHat Las Vegas* (Aug. 4, 2011), *in* ALESSANDRO ACQUISTI, RALPH GROSS, & FRED STUTZMAN, FACE RECOGNITION AND PRIVACY IN THE AGE OF AUGMENTED REALITY (2014), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1122&context=jpc [https://perma.cc/762D-4PX2].

collected, used, or shared for marketing purposes." The constant drip of private and personal data via social media eventually builds up into a detailed profile of who we are, by analyzing our tastes, friendships, habits, opinions and location movements. As we share more the digital world, so we become more vulnerable for the picture to be complete.[124] Perhaps we can look to some of the ways that people try to protect their identity within social networks as a possible paradigm for protecting people from problematic uses of FRT. For example, the emerging right to be forgotten.

FRT AND THE RIGHT TO BE FORGOTTEN

Concerns regarding FRT are very similar to the issues raised by those who support the right to be forgotten.[125] Succinctly it is "based on the fundamental need of an individual to determine the development of his life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action."[126]

Distinct from privacy laws that tend to protect non-public information, right to be forgotten laws protect heretofore public information such as convictions. Similarly, any rights associated with limiting FRT would be some sort of limitation on otherwise public information, such as an image of a pedestrian walking in public.[127]

---

[124] Matthew Wall, *Is Facial Recognition Tech Really a Threat to Privacy?*, BBC TECH. NEWS (June 19, 2015), http://www.bbc.com/news/technology-33199275 [https://perma.cc/F8WS-6UZL].

[125] Albeit the phrasing "the right to be forgotten" is something of a misnomer because it exaggerates the right. *See, e.g.,* Peter Hustinx, Eur. Data Protection Supervisor, The Right to be Forgotten and Beyond: Data Protection and Freedom of Expression in the Age of Web 2.0, Speech at Oxford Privacy Information Law and Society Conference, University of Oxford (June 12, 2012) *in* PETER HUSTINX, THE RIGHT TO BE FORGOTTEN AND BEYOND: DATA PROTECTION AND FREEDOM OF EXPRESSION IN THE AGE OF WEB 2.0 (2012), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2012/12-06-12_Speech_Oxford_EN.pdf ("There is also something of a mistranslation – *le droit á l'oubli* in French is not really the right to be forgotten, so there is an overstatement in the process. We got carried away.").

[126] Alessandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'*, 29 COMPUTER L. & SECURITY REV. 229, 230 (2013).

[127] L. Gordon Crovitz, *Forget Any 'Right to Be Forgotten'*, WALL ST. J., Nov. 15, 2010, at A15 ("Indeed, there's a good argument that 'a "right to be forgotten" is not really a "privacy" right in the first place, . . . A privacy right should only concern information that is actually private. What a "right to be forgotten" does is try to take information that is, by default, public information, and pretend that it's private.'") (quoting Adam Thierer, President, Progress and Freedom Foundation).

The right to be forgotten, arose as a result of the internet's difficulty in forgetting your embarrassing moments. In a widely read blogpost, Peter Fleischer, Google's Global Privacy Counsel, fleshed out the broad spectrum of possible versions of this ideal.[128] Anchored in varied European laws,[129] including, most notably, the French law of le droit à l'oubli, (the right of oblivion) that allowed rehabilitated criminals to prevent the publication of damning evidence of his conviction,[130] and a similar UK law.[131] The Euopean version of the a right to be forgotten law was proposed in 2012 by Viviane Reding, Vice-President of the European Commission, the EU Justice Commissioner,[132] and was accepted by

[128] Peter Fleisher, *The Right to be Forgotten, or how to Edit your History*, PETER FLEISHER: PRIVACY. . .? (Jan. 29, 2012, 6:57 AM), http://peterfleischer.blogspot.co.il/2012/01/right-to-be-forgotten-or-how-to-edit.html [https://perma.cc/UR74-YYPG] ("What is the 'right to be forgotten'? There is a spectrum of views . . . the rights to access and rectify one's own personal data, the right to oppose processing of one's personal data in the absence of legitimate purposes, the principle of data minimization. . . . On the other end of the spectrum, . . . a new right to delete information about oneself, even if published by a third-party, even if the publication was legitimate and the content was true. . . . There is an even more extreme end of the 'right to be forgotten' spectrum, which holds that this deletion right can be exercized not just against the publisher of the content (e.g., a newspaper website), but even against hosting platforms and other intermediaries like search engines that merely host or link to this third-party content.").

[129] Mantelero, *supra* note 126, at 229.

[130] Jeffrey Rosen, *Response: The Right to Be Forgotten*, STANFORD L. REV. ONLINE (Feb. 2012), https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ [https://perma.cc/J695-ZVX6].

[131] *E.g.*, Rehabilitation of Offenders Act 1974, c. 53 §4 (stating that "(1) Subject to sections 7 and 8 below, a person who has become a rehabilitated person for the purposes of this Act in respect of a conviction shall be treated for all purposes in law as a person who has not committed or been charged with or prosecuted for or convicted of or sentenced for the offence or offences which were the subject of that conviction; and, notwithstanding the provisions of any other enactment or rule of law to the contrary, but subject as aforesaid— (a) no evidence shall be admissible in any proceedings before a judicial authority exercising its jurisdiction or functions in Great Britain to prove that any such person has committed or been charged with or prosecuted for or convicted of or sentenced for any offence which was the subject of a spent conviction; and (b) a person shall not, in any such proceedings, be asked, and, if asked, shall not be required to answer, any question relating to his past which cannot be answered without acknowledging or referring to a spent conviction or spent convictions or any circumstances ancillary thereto.").

[132] Viviane Reding, Vice-President of European Comm'n, EU Justice Comm'r, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Speech at the Innovation Conference Digital, Life, Design Munich, (Jan. 22, 2012), *in* VIVIANE REDING, THE EU DATA PROTECTION REFORM 2012: MAKING EUROPE THE STANDARD SETTER FOR MODERN DATA PROTECTION RULES IN THE DIGITAL AGE (2012), http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm

the European Court of Justice,[133] and recommended as part of the EU Data Protection Regulations.[134]

Arguably, the Europeans have long had some form of the right to be forgotten, having many of the underlying tenants reflected elsewhere with the Data Protection Directive.[135] Notably, however while some US courts may have supported a similar idea in the past[136] under current US Supreme Court precedent, such a

[https://perma.cc/M7RY-7Q4Z].

[133] Case C-131/12, Google Spain SL. v. Agencia Española de Protección de Datos (AEPD) 2014, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=29756 [https://perma.cc/P4J7-E63V]. *See* EUROPEAN COMMISSION, FACTSHEET ON THE "RIGHT TO BE FORGOTTEN" RULING (C-131/12*)* (n.d.) http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [https://perma.cc/DL9Z-GR6N] ("Individuals have the right - under certain conditions - to ask search engines to remove links with personal information about them. This applies where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing (para 93 of the ruling). The court found that in this particular case the interference with a person's right to data protection could not be justified merely by the economic interest of the search engine. At the same time, the Court explicitly clarified that the right to be forgotten is not absolute but will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media (para 85 of the ruling). A case-by-case assessment is needed considering the type of information in question, its sensitivity for the individual's private life and the interest of the public in having access to that information. The role the person requesting the deletion plays in public life might also be relevant.").

[134] Procedure 2012/0011/COD § 3, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011 [https://perma.cc/UJV7-XWEX] ("Article 17 provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure provided for in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten, including the obligation of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology 'blocking'").

[135] Paul Bernal, *The EU, the US and Right to be Forgotten, in* RELOADING DATA PROTECTION: MULTIDISCIPLINARY INSIGHTS AND CONTEMPORARY CHALLENGES 61, 62 (Serge Gutwirth et al. eds., Springer 2014).

[136] *See, e.g.*, Melvin v. Reid, 297 P. 91 (Cal. Dist. Ct. App. 1931) (finding that a former prostitute had the right to not have her name connected with her history of prostitution made public in a film after reforming herself); *see also* Briscoe v. Reader's Digest Ass'n, Inc., 483 P.2d 34 (Cal. 1971) (allowing plaintiff, a rehabilitated criminal, to proceed with his right of privacy claim against a publisher who reported on plaintiff's crime from eleven years before); *but c.f.*, Sidis v. F-R Pub. Corp., 113 F.2d 806 (2d Cir. 1940) (finding that the public's interest was an overriding consideration in preventing a news story that discussed the earlier life of the plaintiff, a child prodigy that had sought to live out of the public's eye).

law would be unconstitutional.[137] In the US there would be no expectation of privacy,[138] and legitimate public concern would override the individuals' rights to anonymity.[139] Moreover, actions by private individuals and not the government, e.g., Google, Facebook, and others would not be subject to federal laws, (akin to the EU Data Directive) but rather likely less useful state law, as in the case of Illinois Biometric Information Privacy Act (BIPA).[140]

This distinction between the Europeans and the Americans is useful to drill down on and can be summarized succinctly: in the US there tends to be fewer rights as the government has a relatively laissez faire approach to regulation, but the rights that do exists are more absolute, thus in the US, free speech is the default and there is a substantial burden to override that default. In Europe, as the Brexit campaign will attest, there is zealous (over)regulation,[141] resulting in a plethora of rights, each one relatively weak, but the default is arguably privacy over free speech and unfettered data dissemination.[142]

With these distinctions in mind, it would seem likely that the Europeans might find a right to not be analyzed by racial recognition technology, or at least some sort of right to limit that ability – some control over your public persona. On the flip side, in the US, the rights of the analyzers of faces and their free speech

---

[137] Florida Star v. BJF, 491 U.S. 524, 541 (1989) (holding that "where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed . . . only when narrowly tailored to a state interest of the highest order.").

[138] California v. Greenwood, 486 U.S. 35, 41 (1988) (stating "[a]n individual has no legitimate expectation of privacy in the numbers dialed on his telephone, we reasoned, because he voluntarily conveys those numbers to the telephone company when he uses the telephone. Again, we observed that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'" (quoting Smith v. Maryland, 442 U.S. 735, 743-744 (1979))).

[139] Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975). *See also* Fed. R. Civ. P. 10(a) ("The title of the complaint must name all the parties . . . ."); United States v. Stoterau, 524 F.3d 988, 1012 (9th Cir. 2008) ("[T]he identity of the parties in any action, civil or criminal, should not be concealed except in an unusual case, where there is a need for the cloak of anonymity." (quoting United States v. Doe, 488 F.3d 1154, 1156, n.1 (9th Cir. 2007))).

[140] Katz, *supra* note 73 at 350-51; *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

[141] *See, e.g.,* Louis Rouanet, *Just Another Day in Regulated Europe*, MISES INST. (June 22, 2016, 12:00 AM), https://mises.org/blog/just-another-day-regulated-europe [https://perma.cc/2UHR-TWZX] ("It had been a peaceful night in Europe where all the women are strong, the men are good looking, and the children are above average. Martin woke up on his EU regulated bed and looked through his EU regulated window. This night, Martin had slept like a baby thanks to the 109 EU regulations concerning pillows, the 5 EU regulations concerning pillow cases, and the 50 EU laws regulating duvets and sheets. Martin went to brush his teeth with his toothbrush regulated by 31 EU laws.").

[142] Bernal, *supra* note 135, at 69-70.

rights may trump a citizen's control over data found in the public via publicly placed cameras.

But it is not necessarily that straightforward. In the US there are other rights, equally nearly absolute, that may constrain public, and perhaps even private actors from collecting faceprints or facial recognition that will need to be balanced against the free speech rights.

FRT AND THE RIGHT TO ANONYMITY

Thus, complicating matters is that efforts to limit FRT may not only seek legal precedent from the area of the right to be forgotten, but also from legal efforts to maintain anonymity, which are tied to the First Amendment. And although anonymity is not always good for society(just check the comment section on any website)[143] nevertheless it remains a protected albeit perhaps illusory right:

> It is entirely possible that, even as we speak, the idea that any one of us is ever anonymous-even in a strange city in the middle of a crowd-is an illusion. In terms of anonymity, we may well be back to the days of the village or township. Except that our neighbors now not only know all of our movements, activities and contacts, but they can also look into our yards and have a pretty good idea what's going on in our heads by mining the cookie-crumb trail of electronic detritus that we routinely shed as a concomitant of daily life.[144]

In some legal sense, anonymity may be defined broadly as: "the freedom from being identified and tracked by name while going through the motions of daily life, including physical movement in private and public spaces, the transaction of business online, and the maintenance of personal and professional relationships, habits, and beliefs—however unpopular or repugnant."[145]

Anonymity, even in the public space, protects citizens from the government recording:

> a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . [Tracking of individuals will disclose] trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip

---

[143] Kimberly M. Christopherson, *The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog"*, 23 COMPUTERS IN HUM. BEHAV. 3038 (2007)*; see also* Alex Kozinski, *Two Faces of Anonymity*, 43 CAP. U. L. REV. 1 (2015).

[144] Kozinski, *supra* note 143, at 15.

[145] Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 413 (2014) (citing DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008)).

> club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.[146]

However, unlike the right to be forgotten which is in counterpoise to First Amendment free speech rights, the right to anonymity is arguably a backbone of First Amendment,[147] and efforts to limit anonymous free speech have been found to be unconstitutional.[148] Even anonymous movement is protectable:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'[149]

As such it is clear that anonymity in public is closely related to the right of free association.[150]

Yet the courts remain somewhat confused as to whether there is an actual constitutional right to anonymity[151] and if it exists, to what extent to you have

---

[146] United States v. Jones, 132 S. Ct. 945, 955 (2012) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

[147] Jesse Lively, *Can a One Star Review Get You Sued? The Right to Anonymous Speech on the Internet and the Future of Internet "Unmasking" Statutes*, 48 J. MARSHALL L. REV. 693, 694 (2015) ("Since the revolutionary era, an individual's right to speak and write anonymously has been a component of the First Amendment.").

[148] Talley v. California, 362 U.S. 60, 65 (1960) ("[T]here are times and circumstances when States may not compel members of groups engaged in the dissemination of ideas to be publicly identified."); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (finding Ohio election law prohibiting distribution of anonymous campaign literature, Ohio Rev. Code Ann. § 3599.09(A) (1988), inconsistent with the First Amendment).

[149] *Jones*, 132 S. Ct. at 956 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

[150] *See* NAACP v. Alabama *ex rel*. Patterson, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association . . . .").

[151] *Compare, e.g.*, Brown, *supra* note 145 at 438 ("[T]he Constitution plays no meaningful role in confining the serious anonymity harms associated with FRT technology."), *with, e.g.*, American Knights of the Ku Klux Klan v. Goshen, Ind., 50 F. Supp. 2d 835, 839 (N.D. Ind. 1999) ("The First Amendment embraces the right to communicate and associate anonymously." (citing Buckley v. American Constitutional Law Found., Inc., 525 U.S. 182 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Buckley v. Valeo, 424 U.S. 1 (1976); Talley v. California, 362 U.S. 60 (1960); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958))).

such a right.[152] Judge Kozinski suggests that this ambivalence may reflect society's own ambivalence vis-à-vis anonymity: it's good for me, but I'm not so sure I want you to have it.[153]

Arguably, there is an ongoing circuit split regarding just how much anonymity is protected by the US Constitution. Even those who find anonymity protection within the First Amendment note that the protection provided is far from absolute, particularly for non-political speech.[154] Moreover, even if the First Amendment does provide broad protections to anonymity, barring the Thirteenth Amendment, the US constitution limits government actions, not private ones,[155] and as set out above, facial recognition technology has moved substantially beyond government policing with a multitude of mainstream commercial applications already offering increasingly advanced technologies in this area.

All in all, it would seem that while anonymity may be a promising place to hang a some limitations against abusive use of FRT, the extent of its applicability is severely curtailed. Moreover, even as anonymity remains a fuzzy concept constitutionally, there are more concrete laws that would further seem to imply that, at least in public spaces, the government retains a right to identify you.

ANTI-MASK LAWS AND FRT

There is a wide variety of anti-mask laws in the United States. These laws

---

[152] Kozinski, *supra* note 143, at 16 (citation omitted) (concluding that "[m]y best guess is that there is a limited right to anonymity when it comes to political speech and association, but that right will not trump other concerns - such as anonymous campaign contributions that could be disguised bribes. The question remains whether there is a more general right to anonymity aside from speech or association. My guess is there isn't, at least not in the Constitution. Privacy is protected by the Fourth and Fourteenth Amendments, but it's difficult to find a constitutional anchor for blanket anonymity. While I don't rule out the possibility that such a right will be developed if the appropriate case comes along, it is likely to be a relatively anemic right, if it exists at all.")

[153] Kozinski, *supra* note 143, at 17.

[154] Margot Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP., MEDIA & ENT. L. J. 815, 815 (2013).

[155] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . .They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."); *see also* Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.").

regulate when and how individuals can hide their identity in public. Most recently this came to light during a scourge of clowns in South Carolina,[156] and the threats to arrest them for illegal behavior: "According to South Carolina state law, no one over the age of 16 can appear in public wearing a mask "or other device which concealed his identity."[157]

Anti-mask laws can be considered a practical barometer of the right to anonymity,[158] particularly for those states that do not consider wearing a mask actual speech, but rather as some form of conduct specifically to conceal ones identity in public.[159] Anti-mask laws also raise a number of political and social concerns that are far beyond the scope of this article, but often relate specifically to laws the bar Muslim women from wearing face and identity concealing burqas and veils.[160]

In the United States, a number of states have passed anti-mask laws, with

[156] Katie Rogers, *Creepy Clown Sightings in South Carolina Cause a Frenzy*, N.Y. TIMES (Aug. 30, 2016), http://nyti.ms/2c6a0D4 [https://perma.cc/YDQ6-7265].

[157] Anna Lee, *Police Chief Says Clowns 'Terrorizing Public' Will Be Arrested*, USA TODAY (Sept. 2, 2016, 8:14 AM), http://grnol.co/2bU7VcO [https://perma.cc/W65V-MPN2].

[158] *See, e.g.,* Church of the Ku Klux Klan v. Kerik, 356 F.3d 197, 209 (2d Cir. 2004) ("[T]he Supreme Court has never held that freedom of association or the right to engage in anonymous speech entails a right to conceal one's appearance in a public demonstration. Nor has any Circuit found such a right."); Ryan v. County of DuPage, 45 F.3d 1090, 1096 (7th Cir. 1995) (finding that defendant "Ryan had no right under either the First or the Fourth Amendment to stroll through the DuPage County Courthouse wearing a mask"); American Knights Ku Klux Klan v. Goshen, Indiana, 50 F. Supp. 2d 835, 839 (N.D. Ind. 1999) ("Faced with the task of deciding whether the ordinance violates AKKKK members' First Amendment rights to express themselves and associate anonymously, the court agrees with AKKKK that, on the record presented, it violates that right, and does so unconstitutionally."); Aryan v. Mackey, 462 F. Supp. 90, 92 (N.D. Tex. 1978) (regarding student protesting anonymously: ". . . that the First Amendment does not grant the right to anonymity is correct. The First Amendment grants the right to hold and express views and beliefs. Serious First Amendment questions arise, however, when there is such a nexus between anonymity and speech that a bar on the first is tantamount to a prohibition on the second.").

[159] Notably, in addition to anti-mask laws in the physical space, there are also efforts to have online anti-mask laws, particularly in light of anonymous online bullying and vigilante doxxing to unmask anonymous online posters. *See, e.g.*, Utah HB 255 "Cybercrime Amendments," Availble online at http://le.utah.gov/~2016/bills/static/HB0225.html [https://perma.cc/J297-2EB3] (" modifies the offense of electronic communication harassment to include distribution of personal identifying information"). Arguably, 18 U.S. Code § 119 - Protection of individuals performing certain official duties, would also include doxxing. 18 U.S.C. A. § 119 (2008).

[160] *See* Alice Foster, *Where in the World Are the Burka and Niqab Banned?,* EXPRESS (Sep. 23, 2016), http://www.express.co.uk/news/world/652842/Burka-Niqab-Islamic-Face-veil-Ban-UK-Fine-France-Belgium-Netherlands-Europe-Muslim-dress [https://perma.cc/TCQ2-5JJR].

varying goals and various levels of constitutionality.[161] These range in their goals from limiting citizens ability to mask their identity,[162] to those that seek to prevent masked individuals from deprives others of their rights,[163] or focusing on the commission of or escape from a crime.[164] Courts have been split as to the constitutionality of these statutes.

For example, in Texas, the courts found that the defendant was not guilty of violating the anti-mask statue as the police were able to identify him, even with the mask on and the "the intent of the Legislature [was] to prohibit the wearing in public of any hood or device which would prevent the identity of the wearer from being known."[165] A later court in Texas also found that the state's anti-mask laws were unconstitutional.[166]

Other courts have also found anti-masks laws unconstitutional. For example, in Tennessee, the court found that an ordinance that prohibited Ku Klux Klan members from assembling on MLK day in the City of Pulaski to protest of the Martin Luther King, Jr. National Holiday was unconstitutional in that it limited

---

[161] Kaminski, *supra* note 154, at 848.

[162] *See, e.g.,* GA. CODE ANN. § 16-11-38(a) (2011) (criminalizing wearing "a mask, hood, or device by which any portion of the face is so hidden, concealed, or covered as to conceal the identity of the wearer and is upon any public way or public property or upon the private property of another without the written permission of the owner or occupier of the property to do so"); MINN. STAT. ANN. § 609.735 (West 2009) (prohibiting mask-wearing to conceal identity in a public place unless based on religious beliefs, or incidental to amusement, entertainment, protection from weather, or medical treatment).

[163] *See, e.g.*, CONN. GEN. STAT. ANN. § 53-37a (West 2012) ("Any person who, with the intent to subject, or cause to be subjected, any other person to the deprivation of any rights, privileges or immunities, secured or protected by the Constitution or laws of this state or of the United States, on account of religion, national origin, alienage, color, race, sex, gender identity or expression, sexual orientation, blindness or physical disability, violates the provisions of section 46a-58 while wearing a mask, hood or other device designed to conceal the identity of such person shall be guilty of a class D felony.").

[164] *See, e.g.*, CAL. PENAL CODE § 185 (West 2014) ("It shall be unlawful for any person to wear any mask, false whiskers, or any personal disguise (whether complete or partial) for the purpose of: One—Evading or escaping discovery, recognition, or identification in the commission of any public offense. Two—Concealment, flight, or escape, when charged with, arrested for, or convicted of, any public offense. Any person violating any of the provisions of this section shall be deemed guilty of a misdemeanor.").

[165] Garcia v. State, 443 S.W.2d 847, 848 (Tex. Crim. App. 1969).

[166] Aryan v. Mackey, 462 F. Supp. 90, 94 (N.D. Tex. 1978) (Regarding student anti-Shah demonstrations: "The officials have offered no concrete proof that these students in this demonstration will erupt into the violence that the no-mask regulation is supposed to prevent. Because the connection between the prohibition and the University interest is merely speculative, the regulation cannot stand; for 'in our system, undifferentiated fear or apprehension of disturbance is not enough to overcome the right to freedom of expression.'").

protected speech.[167]

In contrast, some courts have upheld anti-mask statutes as constitutional: for example, in New York, a number of courts have found anti-masks to be constitutional.[168] In Georgia as well, the courts have found anti-mask laws that specifically serve only to prevent people from concealing identity as constitutional.[169] Similarly, the Seventh Circuit found anti-mask statutes that prevented people from wearing masks in court houses to be constitutional.[170]

In the balance of free speech against anonymity, anti-mask laws further tip the scales in favor protected speech and potentially unwanted facial recognition. Perhaps there are other paradigms to support limitations on FRT?

OTHER ETHICAL AND LEGAL CONCERNS ASSOCIATED WITH FRT

Even if FRT cannot be limited due to rights of anonymity or speech, perhaps others will find constitutional challenges associated with discrimination. For example, in contrast to other forms of identification, many also note that FRT will be able to incorporate easily discriminable characteristics such as age, race or gender, social status, religion and even immigration status. This ability raises the concern that some groups may experience even greater levels of price discrimination in the marketplace. Other areas of potential discrimination could arise through the use of FRT in predictive policing algorithms.

Even if you upload and then subsequently delete a photograph online, there are archives and possibly even screenshots of those photos lingering around. Another concerns is that unlike other biometric data like DNA samples or fingerprints that collected only when a person is reasonably seen as a suspect of a crime, photos are frequently collected by a variety of institutions surveillance and security cameras, social internet uploads, library cards and many more. Relatedly, FRT will result in the wholesale objectification of human bodies, objects

---

[167] Ku Klux Klan v. Martin Luther King Worshippers, 735 F. Supp. 745, 751 (M.D. Tenn. 1990) ("[T]he "Pulaski Ordinance is unconstitutionally overbroad because it may be used to stifle symbolic political expression which is protected by the First Amendment."); *but c.f.* Church of Am. Knights Ku Klux v. City of Erie, 99 F. Supp. 2d 583 (W.D. Pa. 2000) (holding that some anti-mask laws were unconstitutionally overbroad, but that other more tailored ones were not.).

[168] People v. Bull, 748 N.Y.S.2d 270, 272 (N.Y. App. Term 2004) (citing Church of the Ku Klux Klan v. Kerik, 356 F.3d 197, 205 (2d Cir. 2004) ("Defendants' constitutional challenges to the anti-mask provisions of Penal Law § 240.35(4) are lacking in merit. The statute, 'aimed at deterring violence and facilitating the apprehension of wrongdoers' upon any First Amendment right to anonymous speech nor constitutes impermissible viewpoint discrimination.")).

[169] State v. Miller, 398 S.E.2d 547 (Ga. 1990).

[170] Ryan v. County of DuPage, 45 F.3d 1090, 1096 (7th Cir. 1995).

whose dimensions are measured, collected and used for purposes that government authorities are not always very clear about. The person isreduced to just a digital algorithm.[171]

Until these issues become more concrete with actual examples of discrimation and other abuses, it is unlikely that the US will develop useful laws that limit FRT. Moreover, with much of the potential laws associated with FRT in flux and inconsistent across the country, and in light of the reality that many of the potentially problematic uses of FRT may not be associated with government actions, there have been efforts by some to develop, in the meantime, a set of best practices for the application of FRT that least impinges on citizens.

THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA) BEST PRACTICES

On June 22, 2016 the US National Telecommunications and Information Administration (NTIA), an agency of the US Department of Commerce, released a set of best practices for the commercial use of facial recognition technologies. The NTIA best practices are based on the widely accepted Fair Information Practice Principles (FIPPs) framework. According to NTIA, the best practices reflect an evolving and flexible approach to FRT uses.

In particular the best practices apply to a "Covered Entity" making commercial uses of facial recognition data. This includes "Any person, including corporate affiliates, that collects, stores, or processes facial template data. Covered entities do not include governments, law enforcement agencies, national security agencies, or intelligence agencies."[172]

The NTIA principles include requirements to:

- Publish policies or disclosures describing their collection, storage, and use of facial template data that include the:
    - reasonably foreseeable purposes for collecting and sharing the data;
    - data retention and de-identification practices; and
    - Individual's ability to review, correct, or delete facial template data.
- Develop internal facial template data management practices that consider:
    - whether the enrollment is voluntary or involuntary;
    - sensitivity of non-facial recognition data also being captured and stored;

---

[171] Ruth E. Gavison, *Privacy and the Limits of Law*, 89 YALE L. J. 421 (1980).

[172] NAT'L TELECOMM. INFO. AND ADMIN., PRIVACY BEST PRACTICE RECOMMENDATIONS FOR COMMERCIAL FACIAL RECOGNITION USE 1 (June 17, 2016), https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf [https://perma.cc/N7XB-XE3K].

  - how they store and use the data;
  - whether the entity will use facial template data to determine a person's eligibility for, or access to, employment, healthcare, financial products or services, credit, housing, or insurance;
  - risks and harms to the individual; and
  - reasonable consumer expectations regarding the data's use.
- Give individuals the ability to control the sharing of their facial template data with unaffiliated third parties.
- Implement reasonable safeguards to protect facial template data.
- Take reasonable steps to maintain the data's integrity and accuracy.
- Establish processes for individuals to contact them about the use of their facial template data.[173]

These best practices recommendations are a result of a two-and-a-half-year process, though they seem to lack both guidance for businesses and protection for individuals.

Most distressingly, a number of non-governmental organizations and stakeholders, including the Electronic Frontier Federation (EFF), The Center for Democracy & Technology (CDT), and other civil society groups, withdrew from the NTIA process, as it became clear to them that the process would not result in meaningful guidelines. The organizations claimed that the Best Practice released impairs the important ability to choose for yourself whether to participate in a face recognition database.[174]

According to the EFF,[175] the companies participating in the NTIA process did not agree that an opt-in system was appropriate in scenarios where unknown third-party companies use FRT to identify and track individuals walking in public streets. The EFF argued further that NTIA's recommendations call into question whether companies will agree to any sort of limitations on their ability to use FRT to track consumers.

Following this action by the NGOs, one industry representative argued that even without the EFF and other privacy and consumer advocacy groups, the company stakeholders "can reach consensus on transparency, notice, data security and giving users meaningful control over the sharing of their facial recognition information with anyone who otherwise would not have access."[176] However, this paper argues that this positon should be treated with caution, given that

[173] *Id.* at 1-3.

[174] Jennifer Lynch, *EFF and Eight Other Privacy Organizations Back Out of NTIA Face Recognition Multi-Stakeholder Process*, ELECTRONIC FRONTIER FOUND. (June 16, 2015), https://www.eff.org/deeplinks/2015/06/eff-and-eight-other-privacy-organizations-back-out-ntia-face-recognition-multi [https://perma.cc/Y56H-VXXF].

[175] *Id.*

[176] *Id.*

without these important NGOs in the process to speak for consumers and the public, consumers will likely lose meaningful control: any multi-stakeholder processes must obtain civil society-industry collaboration.

The NGO walkout notwithstanding, there are key industry stakeholders who are supporting and warmly welcoming the new NTIA best Practices. Alex Reynolds, director of regulatory affairs for the Consumer Technology Association (CTA) is one of the prominent supporters. Reynolds suggests that we should focus on the enormous potential benefits that FRT has to offer, and keep them in balance with carefully crafted privacy protections. "Every new technology raises issues – that's how disruptive innovation works and changes our lives for the better. Privacy discussions continue to evolve, and today's outcome is a milestone – not a stopping point – in the considerate process toward adopting facial recognition technology within the consumer marketplace."[177]

CONCLUSIONS

While the industry continues to use and look for new directions for FRT solutions, legal provisions are not keeping apace with the accelerated technological developments. Companies are left without clear instructions of how to use FRT. As we have witnessed, there is no definite consensus even among the industry and committed stakeholders for different recommendations, leaving us with the anticipation for a clearer but most likely unlikely voice.

It is essential however that the government step up and provide that voice. With all its potential benefits, FRT poses serious challenges to the right for privacy and data security. It creates problems of unwanted identification, discrimination, and the likely hacking of large datasets of not only faces, but also all the data that has been associated with those faces.

While the NTIA effort may be a bust, hopefully their best practices will eventually serve as a template for useful regulations. And the sooner the better.

[177] *Facial Recognition Best Practices Must Balance Innovation and Privacy, Says CTA*, BUSINESS WIRE, (June 15, 2016), http://www.businesswire.com/news/home/20160615006426/en/Facial-Recognition-Practices-Balance-Innovation-Privacy-CTA [https://perma.cc/JX5M-MRSK].