Written Statement
Jonathan Turley,
Shapiro Professor of Public Interest Law
The George Washington University Law School

President's Commission on
Law Enforcement and the Administration of Justice

"*Privacy in the Age of Biometrics*"

Tampa, Florida (Remote)
July 21, 2020

I. INTRODUCTION

Chairman Keith, and Commissioners, my name is Jonathan Turley, and I am a law professor at George Washington University where I hold the J.B. and Maurice C. Shapiro Chair of Public Interest Law.[1] It is an honor to appear before you today to discuss the implications of biometric technology and privacy in law enforcement.

The recent controversies surrounding the defacing and destruction of statues and memorials has led to national debate over the rise of mob action. While there are valid arguments for the removal of some statues, the rule of law demands that these decisions are made collectively by society, not capriciously by rioters. Some incidents in Washington and Baltimore involved the destruction of statues as police made the "tactical decision" not to intervene.[2] The federal government launched an extensive effort to identify the leaders. The same type of effort has unfolded in cities like

---

[1] I appear today on my own behalf and my views do not reflect those of my law school, my colleagues, CBS News, the BBC, or the newspapers for which I write as a columnist.

[2] Jonathan Turley, *People Will Do What People Will Do*, Res Ipsa Blog (www.jonathanturley.org), July 10, 2020 available at https://jonathanturley.org/2020/07/10/people-will-do-what-they-do-pelosi-refuses-to-condemn-statue-destruction/

[3] N'dea Yancey-Bragg, Kristine Phillips & Lindsay Schnell, *"Secret Police Force":*

[2] Jonathan Turley, *People Will Do What People Will Do*, Res Ipsa Blog (www.jonathanturley.org), July 10, 2020 available at https://jonathanturley.org/2020/07/10/people-will-do-what-they-do-pelosi-refuses-to-condemn-statue-destruction/

Portland where federal officers have reportedly attempted to identify protesters who have attacked federal officers or destroyed federal property, including a controversial case where the suspect was detained and then released by officers in an unmarked vehicle.[3]

The recent arrests may or may not have used facial recognition technology (FRT) but they highlight the value and the concerns over the use of biometrics. On one side, there are organized groups who seek to conceal their identity as they engage in mob violence and attacks on police. On the other side, there is the concern over police identifying people who are engaging in protests against their government. Defending the rule of law in stopping such mob action can be as deterring the exercise of rights guaranteed under the rule.

From *1984*[4] to *Total Recall*,[5] fictitious dystopian futures all have a common feature: continual, omnipresent surveillance of every citizen. The fear of living in a fishbowl society is a shared phobia of all free people. The technology that was merely fiction when Orwell penned *1984* now exists to make his dystopian vision a reality. That technology – and that future – has arrived with recent breakthroughs in biometric technology. Biometric technology now inundates society in a myriad of products, including the ubiquitous cellphones with FRT unlocking systems. Billions use and enjoy such products. Governments around the world are incorporating biometric technology at an accelerating pace with widespread deployment of FRT and other systems to identify and track movements of individuals in public.

The exponential growth of this industry has presented an unprecedented tool for law enforcement and an equally unprecedented threat to privacy interests. I have been working on the issue of biometrics and privacy for a number of years. That work is partially reflected in a forthcoming work, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*.[7] I have a second article titled *From Here*

---

[3] N'dea Yancey-Bragg, Kristine Phillips & Lindsay Schnell, *"Secret Police Force": Police Reportedly Pull Portland Protesters Into Unmarked Vehicles*, USA Today, July 17, 2020.

[4] *Id*.

[5] TOTAL RECALL (Tristar Pictures 1990) (Prior to taking a space bridge to the planet Mars, Douglas Quaid, played by actor Arnold Schwarzenegger, proceeds through a full body x-ray scanning machine to detect contraband.).

[7] Jonathan Turley, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics* Jonathan Turley, *Anonymity, Obscurity, and Technology:*

To Obscurity: Conceiving A Biometric Privacy Act for an Anonymous Society that outlines a possible legislative solution in a federal biometric privacy act.

I believe that current legal approaches to both surveillance and privacy are incapable of addressing the issues arising out of biometric technology, particularly FRT. In my view, we will need to not only explore comprehensive international agreements on the use of biometric technology but reexamine our concept of privacy in the age of biometrics. The solution is not to deny this technology to law enforcement but to regulate its use to address legitimate concerns raised over its growing use.

II. BACKGROUND

Given the limitations of time, I will not dwell on the background of biometrics in law enforcement. However, a few points are worth noting. There has been an enormous investment and incorporation of biometrics in other countries, particularly Russia and China, which remain two of the most dominant countries in terms of new technology. The Chinese government is particularly enthralled with this technology for all the wrong reasons. FRT can create the type of "fishbowl" society long feared by civil libertarians and long sought by authoritarian governments. Notably, the greatest concern voiced by protesters in the 2019 protests in Hong Kong was evading FRT systems.[8] Not surprisingly, much of the FRT efforts in China have been directed at ethnic Muslims like the Uighurs and other populations viewed as a threat to the authoritarian regime.[9] With the world's largest network of cameras in public spaces, China was able to incorporate FRT to create a fearsome surveillance system. In one month alone, officials in the city of Sanmenxia screened 500,000 images of Uighurs.[10] Police called it "minority

---

Reconsidering Privacy in the Age of Biometrics, 100 B.U. L. Rev. (forthcoming Dec. 2020). Much of this testimony is taken from this article.

[8] Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, N.Y. TIMES (July 26, 2019), https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.

[9] Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[10] *Id.*

identification," a system that has been denounced for its ability to categorize and identify people based on their ethnicity. Indeed, Chinese companies are now selling programs with "minority recognition functions."[11] China is currently completing the largest FRT system in the world – aimed at identifying all of its 1.3 billion citizens within three seconds with a 90 percent accuracy. Once completed, the already limited ability of citizens in China to engage in protests or reform activities will be sharply reduced. China's interest in FRT is both political and economic. The Chinese and Russians are quickly dominating this international market. Indeed, Microsoft is believed to be using a Chinese algorithm.

The United States has also made significant investments in FRT. In 2017, the government used FRT at nine airports for its Biometric Entry-Exit Program. Biometric e-gates are operating at LAX in California, New York's JFK Airport, Orlando International in Florida, and other airports.[17] TSA test programs are now being used in airports like Las Vegas.[18] This biometric system was not only funded as part of the Consolidated Appropriations Act of 2016 but also ordered to be implemented by Executive Order 13780.

In addition to the entry-exit program, various agencies already utilize biometric technology with a massive collection of data. The Federal Bureau of Investigations (FBI) recently disclosed that it has 641 million facial images in its databank associated with the Facial Analysis, Comparison, and Evaluation (FACE) program. Almost 40 million such images were taken from the FBI's Interstate Photo System of mugshots. The rest were mined from databanks ranging from passport to driver license files. The FBI's Next Generation Identification (NGI) is moving ahead with little regulation from the Congress. Likewise, the Department of Defense (DoD) implemented a highly advanced Automated Biometric Identification System (ABIS) that interacts with other databanks and can cross-check facial recognition, palm prints, fingerprints, irises, and other biometric data on individuals. The domestic incorporation of this FRT extends to municipal and law

---

[11] *Id*.

[17] Sean O'Kane, *British Airways brings its biometric identification gates to three more US airports*, VERGE (Mar. 9, 2018, 12:17 PM), https://www.theverge.com/2018/3/9/17100314/british-airways-facial-recognition-boarding-airports.

[18] Brandi Vincent, *TSA Launches Facial Recognition Pilot at Las Vegas Airport*, NEXTGOV (Aug. 27, 2019), https://www.nextgov.com/emerging-tech/2019/08/tsa-launches-facial-recognition-pilot-las-vegas-airport/159479/.

enforcement departments, like the New York Police Department, which is currently storing pictures of individuals as young as eleven years old.[19]

The dangers of this technology are not just limited to privacy loss. There are been serious concerns raised over racial discriminatory results, particularly with persons of color. For many years, the industry has struggled with false identifications that continue to concern many of us over the accuracy and application of the technology.

Conversely, biometrics offers obvious benefits to law enforcement that cannot be dismissed. Consider the Boston Bombing where police declared a "containment zone" and forced families into the street with their hands in the air.[22] The suspect, Dzhokhar Tsarnaev, was ultimately found outside the "containment zone" once authorities abandoned near martial law. Once people were allowed out of their homes and with millions of new eyes on the street, Tsarnaev was quickly spotted hiding in a boat. In such a situation, FRT can help law enforcement avoid time consuming area searches and the questionable practice of forcing people out of their homes to physically examine them. As Tsarnaev and his brother traveled around Boston, FRT systems might have identified them and ultimately avoided such draconian measures.

It is also important to recognize that biometrics can have privacy benefits. When properly used, they can enhance privacy interests and even reduce racial profiling by reducing false arrests and unwarranted Terry stops.[23] Consider again the Portland controversy. FRT can radically increase the chances that the person detained was actually the person being sought by the federal officers. Bans like the one in San Francisco not only deny police a technology widely used by businesses, but returns police to the highly flawed default of "eye balling" suspects where the error rate is considerably higher than top FRT programs. A study in Australia offers a glimpse into the

---

[19] Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, N.Y. TIMES (Aug. 1, 2019), https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

[22] Jonathan Turley, *The Pavlovian Politics of Terror*, JONATHANTURLEY.ORG (Apr. 29, 2013), https://jonathanturley.org/2013/04/29/the-pavlovian-politics-of-terror/comment-page-4/.

[23] A similar debate arose over the use of body cameras. *See* Floyd v. City of New York, 959 F. Supp. 2d 668, 685 (S.D.N.Y. 2013) (noting that the use of body camera "will provide a contemporaneous, objective record of stops and frisks.").

performance differential between human and FRT recognition.[24] A study of passport officers showed high error rates, including fourteen percent false acceptance rates in testing. What was striking was that the test used photos taken just two days before (and in optimal settings) the testing subjects appeared before the officers. The variables of aging and poor images were therefore not present to the same degree as real life. Nevertheless, the error rate was high with an overall matching rate of only seventy percent.[25] This was in a controlled environment with both the subjects and good quality photos in front of the officers, as opposed to a street with varying lighting and recollection of a prior image.

Finally, the suggestion that we can stop the use and expansion of this technology is naïve. This is a hugely popular technology that is already part of a multi-billion industry. To put it simply, there is no way to get this cat to walk backwards. We may, however, be able to get this cat to walk down a path that we lay to balance the interests of law enforcement and privacy.

III. PRIVACY IN THE BIOMETRIC AGE

The rapid expansion of this technology has collided with a body of law that has changed little conceptually from early eavesdropping cases in defining privacy protections. FRT and biometric technology presents a quantum shift for privacy theory. Since FRT occurs in public, it falls into an area long treated as having minimal expectations of privacy. Indeed, it is technology that is perfectly suited to evade privacy protections. For those worried about a post-privacy world, FRT and biometrics could well be the expanding portal to that dystopia. That technology implicates the loss of freedom to move and interact in public space without fear of being recognized or tracked. That loss impacts the ability of individuals to freely form new experiences, associations, and viewpoints.

The result is that the two sides have adopted the most extreme positions. Privacy advocates have called for total bans which will never occur while some FRT developers and investors have dismissed privacy as a dated concept outstripped by technology.[28] The question is whether

---

[24] David White, Richard Kemp, Rod Jenkins, et al., *Passport Officers' Errors In Face Matching*, PLOS One, August 19, 2014.

[25] *Id.* at 3.

[28] Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, The New York Times, Jan. 18, 2020 (Investor David Scalzo with Kirenaga Partners quoted in 2020 as saying "I've come to the conclusion that because information

technology and privacy are now part of are now, truly a zero-sum games. I do not believe they are.

If left to traditional views of privacy (including its general rejection of the concept of "public privacy"), biometric technology could expand exponentially and create the type of "fishbowl" or post-privacy world that civil libertarians have long feared. Instead, I suggest that the focus of biometric privacy should be the protection of democratic values of speech and association in public. Specifically, we need to focus on anonymity rather than privacy in seeking judicial and legislative solutions. Anonymity comes closer to capturing the value that we seek to protect: allowing people to move in public without recognition or potential tracking. As noted, the problem with anonymity as the focus for biometric privacy is that we are increasingly living in a nonymous rather than anonymous society. This is due to a myriad of products and practices embraced by consumers that use FRT and biometric technology. Accordingly, I suggest that it is not anonymity but obscurity that should be the focus of biometric privacy. The idea is that we can protect democratic values of public association and interactions by obscuring recognition even in an otherwise nonymous society. In this way, a right to obscurity in public movements can help create and maintain the type of "bounded rationality" needed for democratic expression and associations.

This is why I suggest a comprehensive legislative approach that regulates the use of this technology, including criminal provisions. They include the use of warrants for FRT searches as well as regulations on the storage and sharing of images. An analogy is drawn to the drafting of omnibus law on electronic surveillance, which came after the Supreme Court defined privacy protections with the expansion of electronic surveillance. Biometric technology requires an even more fundamental reconsideration of the interests that we need to protect in public, including "anonymity by obscurity" in public movements and associations.

The creation of a Biometric Privacy Act can rely on the limited relevant decisions on biometrics the way that Congress did after the Supreme Court's rulings on electronic surveillance. In *Berger v. New York,*[29] the Court reviewed the New York surveillance law and found

---

constantly increases, there's never going to be privacy. Laws have to determine what's legal, but you can't ban technology. Sure, that might lead to a dystopian future or something, but you can't ban it.").

[29] Berger v. New York, 388 U.S. 41 (1967).

various constitutional deficiencies that were then used as the foundation for Title III of the Omnibus Crime Control and Safe Streets Act, which was enacted into law. The specific provisions of such an Act are the focus of another work.[30] However, a few broad components of a Title 55 for biometric privacy are worth emphasizing.

As a threshold matter, any effort to create a protected space for biometric privacy would require the preemption of state laws. The Illinois Biometric Information Privacy Act (BIPA)[31] is a leading example of state experimentation in regulating this expanding market. Texas[32] and California[33] also have enacted laws with state limits and liabilities. As with command and control statutes like the Clean Air Act and market-based statutes like the Sherman Act, biometric privacy is an interstate problem demanding a single national approach. Biometric technology is used on the Internet and has a classic interstate profile for regulation by Congress. The worst possible approach to regulation is the creation of a patchwork of different state laws with different approaches to privacy protections.

A Biometric Privacy Act would have to include both limits on public and private uses of FRT and biometric technology. While the Supreme Court should extend Fourth Amendment protections to biometric searches with the attendant requirement of a warrant, Congress can also require such protections as it did with Title III. In this way, law enforcement would be allowed to have FRT and biometric capabilities but would require the showing of probable cause to use this technology to find a wanted felon. Thus, if the police have probable cause supporting the identification of a murder suspect, it could secure a court order to allow access to live FRT systems in locating the individual in public. A law would also stipulate conditions and protections governing government biometric databanks, limiting access and barring the transfer of data absent the satisfaction of defined conditions. A national legislative solution would also need to create a compatible regulatory platform with recent European regulations of biometric technology. There is currently a vacuum created by the lack of any comprehensive U.S. law on biometrics.

---

[30] Turley, *From Here To Obscurity*, *supra* note 73.

[31] 740 ILL. COMP. STAT. 14/1-14/99 (2008).

[32] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

[33] CAL. CIV. CODE § 1798.198(a) (West 2018).

An EU-compatible act would also allow FRT and biometric technology to be used more effectively for identity authentication. While often portrayed as a technology inimical to individual rights and privacy values, FRT and biometric technology could play a critical role in greatly reducing identity theft and other crimes. Likewise, an act could further strengthen international standards for products to address concerns over erroneous identifications based race and gender.

I have proposed the outlines of a biometric privacy act that would protect individuals in their public movements and associations as well as their Internet associations.[34] However, before such protections are debated, we need to clearly define what we are protecting and why. The democratic value of anonymity cannot be seriously denied. The question is how to protect those democratic values when society is turning away from anonymity. The answer that I propose is to build FRT and biometric privacy protections around the model of obscurity. It is possible in a nonymous society to codify a level of obscurity (as opposed to anonymity). After all, the most important interest in anonymity is the protection of the democratic process and engagement.[35] By codifying a type of "anonymity by obscurity," we can create the guarantee sought by many citizens that the government will be allowed to gather recognition data on public events without a tailored and specific warrant seeking an individual.[36]

Such protections are premised on the basic need for human development and democratic processes to be obscure. FRT threatens to reproduce the "Hawthorne Effect"[37] exponentially – changing how not just

---

[34] Jonathan Turley, *From Here To Obscurity: Conceiving A Biometric Privacy Act for an Anonymous Society* (forthcoming 2019).

[35] In the balancing of interests with privacy, the importance of privacy to the democratic process has rarely been weighted by courts or commentators. *But see* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 50 (2011); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 7 (2003).

[37] The Hawthorne effect was named after an experiment at the Hawthorne factory in Chicago in 1924. The owners wanted to see if the level of lighting impacted productivity and, if so, what level of lighting was optimal. The research found a direct correlation to observation on human behavior, something he called "the Hawthorne Effect." *See* Steven D. Levitt & John A. List, *Was There Really A Hawthorne Effect at the Hawthorne Plant? An Analysis of the Original Illumination Experiments*, 3 AM. ECON. J. APPLIED ECON. 224, 229-36 (2011).

how citizens act but interact. Even the possibility of constant recognition and tracking can have a pronounced impact on personal development. Put another way, people have always lost themselves in a crowd. That invisibility allows them to observe in a way that would be chilled by observation.

With the onslaught of transparency-forcing technology, it is not clear if we can go back to true anonymity by obscurity in society. However, we can make recognition less chilling by limiting the use and sharing of biometric data by private and government parties. That may be the best that can be done when citizens themselves are surrendering anonymity. Presented with increasing threats of identity theft (and a poor government record in combating such crime), citizens view FRT and biometric technology as a way of protecting their own identities. As a result, recognition technology is becoming a part of modern life as privacy continues to evolve with social norms.

III. CONCLUSION

FRT and biometric technology presents an obvious threat to privacy and the political process. The technology promises transformative change in both legal and social realities for citizens. It will force us to deal with what we are working to protect in public forums. This is a distinctly descriptive or instrumental approach to privacy. However, it can better understand the specific threat of this technology that can be lost in the thrill of recognition programs from cellphones to airport security gates. The success of biometric products in society will soon become a menace to society if we cannot reach a consensus on what we can protect and how we can protect it.

Any progress on biometric privacy will require a comprehensive re-examination of what interests we are seeking to protect in our new nomymous world, including the limits of traditional privacy definitions. If that zone of safe interaction and exploration is lost, the impact on society – particularly democratic societies – could be as transformative as it is tragic.

Once again, thank you for the honor of appearing before you to discuss this important issue. I am happy to answer any questions that you might have on the underlying legal standards that apply to this controversy.

Jonathan Turley
J.B. & Maurice C. Shapiro Chair of Public Interest Law
George Washington University