Richmond Public Interest Law Review

Volume 26
Issue 1 *General Assembly in Review 2022*

Article 8

1-17-2023

From Ban to Approval: What Virginia's Facial Recognition Technology Law Gets Wrong

Alison Powers

Korica Simon

Jameson Spivack

Follow this and additional works at: https://scholarship.richmond.edu/pilr

Part of the Public Law and Legal Theory Commons

Recommended Citation

Alison Powers, Korica Simon & Jameson Spivack, *From Ban to Approval: What Virginia's Facial Recognition Technology Law Gets Wrong*, 26 RICH. PUB. INT. L. REV. 155 (2023).
Available at: https://scholarship.richmond.edu/pilr/vol26/iss1/8

This Article is brought to you for free and open access by the Law School Journals at UR Scholarship Repository. It has been accepted for inclusion in Richmond Public Interest Law Review by an authorized editor of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.

FROM BAN TO APPROVAL: WHAT VIRGINIA'S FACIAL RECOGNITION TECHNOLOGY LAW GETS WRONG

Alison Powers[*], *Korica Simon,*[**] *& Jameson Spivack*[***]

[*] Alison Powers is the Director of Policy and Education at the Virginia Indigent Defense Commission (VIDC). Alison has been with the VIDC since 2010. She worked for seven years as an Assistant Public Defender at the Office of the Public Defender in Fairfax, Virginia, handling hundreds of cases in General District Court, Juvenile and Domestic Relations District Court, and Circuit Court. In 2018 she moved to the administrative office where she manages the VIDC's legislative team and all training for VIDC attorneys, staff, and court appointed counsel. Alison earned a J.D. from the UCLA School of Law where she served as co-Editor in Chief of the Los Angeles Public Interest Law Journal. Prior to law school, Alison graduated with Highest Honors from Emory University.

[**] Korica Simon is an Associate at the Center on Privacy & Technology at Georgetown Law. Previously, she worked at the Monroe County Public Defender's Office as an Assistant Public Defender. Korica earned a J.D. from Cornell Law School, where she served as an Acquisitions Editor for the Cornell Journal of Law and Public Policy.

[***] Jameson Spivack is Senior Policy Analyst, Immersive Technologies at Future of Privacy Forum. He formerly served as an Associate with the Center on Privacy & Technology at Georgetown Law, where he studied algorithmic technologies like face recognition in the criminal legal system.

ABSTRACT

Face recognition technology (FRT), in the context of law enforcement, is a complex investigative technique that includes a delicate interplay between machine and human. Compared to other biometric and investigative tools, it poses unique risks to privacy, civil rights, and civil liberties. At the same time, its use is generally unregulated and opaque. Recently, state lawmakers have introduced legislation to regulate face recognition technology, but this legislation often fails to account for the complexities of the technology, or to address the unique risks it poses. Using Virginia's recently passed face recognition law and the legislative history behind it as an example, we show how legislation can fail to properly account for the harms of this technology.

INTRODUCTION

Face recognition technology (FRT), in the context of law enforcement, is a complex investigative technique that includes a delicate interplay between machine and human. Compared to other biometric and investigative tools, it poses unique risks to privacy, civil rights, and civil liberties. At the same time, its use is generally unregulated and opaque. Recently, state lawmakers have introduced legislation to regulate face recognition technology, but this legislation often fails to account for the complexities of the technology, or to address the unique risks it poses. Using Virginia's recently passed face recognition law and the legislative history behind it as an example, we show how legislation can fail to properly account for the harms of this technology.

Section I will discuss FRT generally, how a FRT search is run, and its reliability. Section II will focus on the legislative history of FRT in Virginia culminating with the authorization of the use of FRT by local law enforcement and campus police in 2022. Finally, Section III will discuss how Virginia's law does not adequately address the risks of FRT.

I. FACE RECOGNITION TECHNOLOGY: BACKGROUND AND QUESTIONS OF RELIABILITY

FRT is a complex technique that involves both machine and human.[1] As such, in order to achieve scientific validity, its performance must be

[1] Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Ctr. Priv. & Tech. Geo. L. 1, 7 (2022), https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf.

evaluated within the specific contexts in which it is used—not merely as an algorithm in isolation, but as part of an investigative process. Yet in the context of policing, FRT has never been comprehensively studied, and its baseline reliability as an investigative law enforcement tool has not been established.[2] Numerous studies have evaluated the accuracy and demographic performance differences (bias) of face recognition algorithms, finding a large gap between the top-performing algorithms and the lowest-performing algorithms, which still exhibit problems with accuracy and race, gender, and age bias.[3] However, while algorithmic accuracy is a crucial component of overall face recognition performance, these studies do not examine how police actually use the technology in practice, which is critical to understanding its performance and potential harms.[4]

A. THE PROCESS OF A POLICE FACE RECOGNITION SEARCH

To better understand the sociotechnical nature of FRT, it is helpful to examine how the technique is actually used in police investigations. Typically, police use face recognition to identify a person in a photograph.[5] In the first step of a face recognition search, police choose which photograph to run, which is known as the "probe" photo.[6] Next, police may have the ability to decide which database of face images to run a search against as a comparison to the probe photo. Often this decision is made when a face recognition system is first implemented, rather than each time a search is run. The database is important because it impacts who is identified as the result of a search,[7] the

[2] *Id.* at 31-32.

[3] *See generally* PATRICK GROTHER ET AL., FACE RECOGNITION VENDER TEST PART 3: DEMOGRAPHIC EFFECTS, NAT'L INST. OF STANDARDS & TECH. (2019) https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (explaining that accuracy of facial recognition varies across demographics); Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, MDTF, https://mdtf.org/publications/demographic-effects-image-acquisition.pdf (last visited Nov. 10, 2022) (publication can also be found at 1 IEEE TRANSACTIONS ON BIOMETRICS, BEHAV., AND IDENTITY SCI. 32 (2019), DOI: 10.1109/TBIOM.2019.2897801) (providing data points on the relationship between demographics and facial recognition technology).

[4] Garvie, *supra* note 1, at 36-41.

[5] *See generally* Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ (providing the statistics on photo usage by police departments across the country).

[6] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data,* GEO. L. CTR. ON PRIV. AND TECH (May 16, 2019), https://www.flawedfacedata.com. The quality of the photo, including pixelation, lighting, and face pose all impact the search's reliability; thus, photo choice is an important aspect of accuracy. *See* Patricia Alejandra Pacheco Reina et al., *Understanding the Impact of Image Quality in Face Processing Algorithms*, PROC. OF THE INT'L CONF. ON IMAGE PROCESSING AND VISION ENG'G 145, 149 (2021), https://www.scitepress.org/Papers/2021/104865/104865.pdf; *see also Facial Comparison Overview and Methodology Guidelines*, FISWG 5 (Oct. 25, 2019), https://fiswg.org/fiswg_facial_comparison_overview_and_methodology_guidelines_V1.0_20191025.pdf.

[7] Only those people included in a database can turn up as a result. For example, a database of mugshot photos will only return those who have been arrested. Garvie, *supra* note 1, at 11.

quality of the photos,[8] and potential misidentification rates.[9]

Once a police officer has selected a photo and database, they may edit the photo to better align its appearance with the database photos. This can include changing size, lighting, and pixelation, or even more significant alterations such as copying and pasting features from other faces, combining photos, or using modeling to approximate features.[10] After editing, the officer submits the photo to an algorithm, which creates a template of the face in question and compares this to templates of face photos in the chosen database.[11] The algorithm then produces a list of potential matches with an accompanying score based on how confident the algorithm is of a match.[12] The confidence score can be adjusted up or down by the user to either restrict or expand the number of results returned by the algorithm.[13]

Once the search has been run, police decide what to do with the results. First, the officer must look at the list of possible matches and determine whether any of them represent actual potential matches. This is done by visually comparing the suspect's initial probe photo with the photos provided by the algorithm.[14] Finally, once possible matches are selected, police theoretically must conduct a follow-up investigation to collect corroborating evidence. Most police departments consider—or claim to consider—the results of a face recognition search as merely an investigative lead.[15] However, there is no guidance about what constitutes corroborating evidence, and in the absence of this, police have used face recognition as sole or primary evidence to establish probable cause for arrest.[16]

B. THE RELIABILITY OF POLICE FACE RECOGNITION HAS NOT BEEN ESTABLISHED

As the above section illustrates, "face recognition" refers not merely to an algorithm by itself, but an investigative technique with numerous parts.

[8] A database with older photos, or lower-quality photos, will be less reliable. *See Standard Guide for Capturing Facial Images for Use with Facial Recognition Systems*, FISWG, 3-4 (Mar. 10, 2019), https://fiswg.org/FISWG_Guide_for_Capturing_Facial_Images_for_FR_Use_v2.0_20190510.pdf.

[9] The larger the database, the more potential matches. However, there's also a greater chance there will be people who look similar, driving up misidentification rates. *See Understanding and Testing for Face Recognition Systems Operation Assurance*, FISWG 4-5 (Dec. 11, 2020), https://fiswg.org/fiswg_understanding_&_testing_for_frs_operatnl_assur_v1.0_2020.12.11.pdf.

[10] *Facial Recognition Systems: Methods and Techniques*, FISWG 8-9 (May 16, 2013), https://www.fiswg.org/FISWG_fr_systems_meth_tech_v1.0_2013_08_13.pdf; Garvie, *supra* note 6.

[11] Garvie, *supra* note 1, at 25.

[12] *Id.;* Garvie et al., *supra* note 5.

[13] Garvie, *supra* note 1, at 25.

[14] The ability to identify faces of strangers is highly variable, not particularly strong, and lacks standardized training for police in the US. *Id.* at 26.

[15] *Id.* at 27.

[16] *Id.*

While the performance of face recognition algorithms in isolation has been evaluated,[17] and the innate ability of humans to recognize faces has been tested,[18] police use of face recognition as an overall investigative technique has not been sufficiently studied, and its reliability has not been established.[19] As such, its use in the context of law enforcement remains questionable. In fact, due to issues present in both face recognition algorithms and human face identification, it may never be possible to truly establish reliability.[20]

At the algorithm level, face recognition exhibits two barriers to establishing reliability: 1) there is a high degree of variability in performance across algorithms, and 2) even individual algorithms perform differently depending on the person being searched.[21] Researchers at the National Institute for Standards and Technology (NIST) evaluated the accuracy of commercially-available face recognition algorithms and found that the false negative rate—when an algorithm indicates two faces are not a match when they actually are—can vary from under 1% to over 50%, depending on the algorithm used.[22] Algorithm performance depends on factors such as quality of data on which it was trained, the strength of the algorithm's training, and other design choices.[23] At the same time, even the same algorithm might perform better or worse depending on the photograph being run, since an algorithm's accuracy depends on factors such as photo quality and the demographics of the person in the photo.[24] As has been extensively documented, a face recognition algorithm may perform differently depending on a person's race, sex, or age, with biased algorithms most often performing worse on people with dark skin, women, and younger people.[25]

These two parallel phenomena make it difficult, if not impossible, to establish a baseline understanding of how reliable a given face recognition search is. Such an understanding is a key component of rigorous investigative techniques and is necessary for human operators (such as police) to make decisions based on the results of face recognition searches. As the President's

[17] *See, e.g.*, GROTHER ET AL., *supra* note 3, at 1.; Cook et al., *supra* note 3, at 1.

[18] *See* Vicki Bruce et al., *Matching Identities of Familiar and Unfamiliar Faces Caught on CCTV Images*, 7 J. OF EXPERIMENTAL PSYCH. 207, 207 (2001); Matthew C. Fysh & Markus Bindemann, *Human-Computer Interaction in Face Matching*, 42 Cognitive. Sci. 1714, 1714 (2018).

[19] Garvie, *supra* note 1, at 34.

[20] *Id.* at 70.

[21] PATRICK GROTHER, ET AL., FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION, NAT'L INST. OF STANDARDS & TECH. 11 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf \; Garvie, *supra* note 1, at 37, 41.

[22] GROTHER ET AL., *supra* note 21, at 6.

[23] Garvie, *supra* note 1, at 36; GROTHER ET AL., *supra* note 21, at 5.

[24] GROTHER ET AL., *supra* note 21, at 7.

[25] GROTHER ET AL., *supra* note 21, at 8.; Cook et al., *supra* note 3, at 1. For more in depth discussion about algorithmic performance variations, *see infra* Section III.

Council of Advisors on Science and Technology (PCAST) reported, "without appropriate estimates of accuracy [of a given forensic investigative technique], an examiner's statement that two samples are similar…is scientifically meaningless; it has no probative value."[26] When algorithmic performance is so variable, across *and* between algorithms, officers have no foundation for understanding how accurate the results of a search are.[27]

Likewise, the human aspect of face recognition—such as comparing possible matches and deciding whom to investigate—suffers from several issues that call into question the reliability of the overall technique. First of all, the vast majority of humans are inherently poor at identifying and comparing strangers' faces.[28] When a police officer compares the results of a face recognition search to the photo of the suspect, they must decide whether any of the possible matches warrant further investigation, and this decision will be impacted by their probable inability to accurately identify strangers' faces.[29]

Likewise, the human aspect of face recognition—such as comparing possible matches and deciding whom to investigate—suffers from several issues that call into question the reliability of the overall technique. First of all, the vast majority of humans are inherently poor at identifying and comparing strangers' faces.[30] When a police officer compares the results of a face recognition search to the photo of the suspect, they must decide whether any of the possible matches warrant further investigation, and this decision will be impacted by their probable inability to accurately identify strangers' faces.[31]

Additionally, most officers who run face recognition searches lack any training in forensic face comparison.[32] While there are trainings that *may* help reduce the impact of human error in face comparison,[33] many police

[26] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., REPORT TO THE PRESIDENT: FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS 6 (2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

[27] Garvie, *supra* note 1, at 36-37.

[28] *See* Bruce et al., *supra* note 18, at 207; Fysh & Bindemann, *supra* note 18, at 1715; David White et al., *Error Rates in Users of Automatic Face Recognition Software*, PLoS ONE, Oct. 14, 2015, at 1, 2; A. Mike Burton et al., *Face Recognition in Poor-Quality Video: Evidence From Security Surveillance*, 10 PSYCH. SCI. 243 (1999).

[29] The inability to recognize strangers' faces also gets worse depending on the photo's lighting and quality and the pose of the person in question. *See* Garvie, *supra* note 1, at 26; Garvie, *supra* note 6; Burton et al., *supra* note 28.

[30] *See* Bruce et al., *supra* note 18, at 207; Fysh & Bindemann, *supra* note 18, at 1715; White et al., *supra* note 28; Burton et al., *supra* note 28.

[31] The inability to recognize strangers' faces also gets worse depending on the photo's lighting and quality and the pose of the person in question. *See* Garvie, *supra* note 1, at 26; Garvie, *supra* note 6; Burton et al., *supra* note 28.

[32] *See* Garvie et al., *supra* note 5.

[33] *Guide for Role-Based Training in Facial Comparison*, FISWG 1 (July 17, 2020), https://fiswg.org/fiswg_guide_for_role-based_training_in_facial_comparison_v1.0_20200717.pdf.

departments do not follow these guidelines.[34] In fact, there is little to no consensus about what constitutes effective training in face comparison in the first place.[35] The generally recommended practices do not guarantee that the technique is reliable; according to PCAST, "neither experience nor professional practices can substitute for foundational validity."[36]

Not only are humans innately bad at identifying the faces of strangers, they also suffer from a number of cognitive biases that further impede their ability to make sound judgments related to forensic face comparison.[37] For example, contextual information about details of the investigation—such as the race or sex of the suspect or victim, the crime in question, or knowledge of a suspect's criminal history—may bias an officer's face comparisons.[38] Similarly, officers can suffer from confirmation bias, in which they interpret information (such as the results of a search) in a way that aligns with previously-held theories and beliefs.[39] Other biases—such as a motivation to provide closure on a case[40] or a mistaken belief in the infallibility of forensic investigators[41]—may also impact their judgment. While these are not unique to FRT, it is notable that FRT is used, generally, in the absence of protocols, guidelines, and standards.[42] Even cases in which FRT is "regulated"—including under Virginia's most recent law—often fail to truly address the issues with the technique.[43]

C. A LACK OF BOTH RELIABILITY AND STANDARDS HAS LED TO WRONGFUL ARRESTS

Partly because neither baseline reliability nor standards for use have been

[34] Garvie, *supra* note 1, at 54.

[35] *Id.* at 53.

[36] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., *supra* note 26, at 55.

[37] Garvie, *supra* note 1, at 59-60; Paul Giannelli, *Independent Crime Laboratories: The Problem of Motivational and Cognitive Bias*, 2010 UTAH L. REV. 247, 252 (2010); PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., *supra* note 26, at 31.

[38] MJ SAKS ET AL., *Context Effects in Forensic Science: A Review and Application of the Science of Science to Crime Laboratory Practice in the United States*, 43 SCI. & JUST. 77, 78 (2003); SAUL M. KASSIN ET AL., *The Forensic Confirmation Bias: Problems, Perspectives, and Proposed Solutions*, 2 J. OF APPLIED RSCH IN MEMORY & COGNITION 42, 43 (2013).

[39] Raymond S. Nickerson, *Confirmation Bias: A Ubiquitous Phenomenon in Many Guises*, 2 REV. OF GEN. PSYCH. 175, 191 (1998); John J. Howard et al., *Human-algorithm Teaming in Face Recognition: How Algorithm Outcomes Cognitively Bias Human Decision Making,* PLOS ONE, Aug. 21, 2020, at 1, 8 (2020).

[40] Giannelli, *supra* note 37, at 251.

[41] *Id.* at 254.

[42] Garvie, *supra* note 1, at 21, 91.

[43] *Id.* at 69, 90.

established, FRT has led to misidentifications and wrongful arrests.[44] Not only is there often nothing stopping police from engaging in questionable search practices, such as heavily editing images or running celebrity lookalike photos,[45] there is also no guidance on what additional evidence beyond the results of a face recognition search is sufficient for an arrest warrant.[46] As a result, police have made arrests based either solely or primarily on results of FRT searches.[47] In a number of publicly known cases, these arrests turned out to be wrongful—the results of FRT misidentifications.[48] Notably, all those wrongfully arrested were Black men, illustrating the disparate impact of FRT use and misidentifications.[49]

D. FACE RECOGNITION POSES NUMEROUS RISKS BEYOND QUESTIONS OF ACCURACY AND BIAS

Beyond issues of accuracy and bias, FRT poses unique privacy risks because it changes the balance of power between the government—particularly police—and civilians. It allows police to surveil large groups of people secretly, from a distance, and without getting a warrant.[50]

FRT searches can be made in the absence of any degree of suspicion, and the inclusion of a person's face image in an FRT database is often done without consent.[51] The constitutionality of FRT is also questionable: in 2018, the Supreme Court ruled that people's locations and movements over time in

[44] The lack of standards has also led to the heavy manipulation of probe photos during preprocessing, celebrity lookalike photos being run as probe photos, inaccurate and biased algorithms being used, poor quality photos being used as probe photos, officers without training using FRT, and the results of FRT searches being used as the sole or primary basis for probable cause to arrest. *Id.* at 94; Garvie, *supra* note 6.

[45] In 2017, while investigating a report of a theft, New York Police Department officers ran a photo of Woody Harrelson through a face recognition system, after the initial search—which was done on the actual suspect's photo—returned no matches. Garvie, *supra* note 6.

[46] *Id.*

[47] Garvie, *supra* note 1, at 16.

[48] Garvie, *supra* note 1, at 58; Supreme Court of the State of New York The People of the State of New York v. Defendant, Notice of Motion to Suppress (redacted) (N.Y.); Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/; Complaint at ¶ 29, Parks v. McCormack et al., Case no. 2:2021cv04021, (D.N.J. 2021); Aff. of Probable Cause, New Jersey v. Parks (Woodbridge Mun. Ct. 2019) (No. 19010123); Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, DETROIT FREE PRESS (July 10, 2020), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

[49] Garvie, *supra* note 1, at 73; Supreme Court of the State of New York The People of the State of New York v. Defendant, Notice of Motion to Suppress (redacted) (N.Y.); Hill, *supra* note 48; Johnson, *supra* note 48; Complaint at ¶ 29, Parks v. McCormack et al. (D.N.J. 2021); Aff. of Probable Cause, New Jersey v. Parks (Woodbridge Mun. Ct. 2019) (No. 19010123); Anderson, *supra* note 48.

[50] Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.americaunderwatch.com/.

[51] Garvie, et al., *supra* note 5.

public spaces reveal sensitive information, and therefore police need to get a search warrant to track that information.[52] While the court has never ruled on face recognition specifically, it is reasonable to apply this reasoning to FRT for surveillance purposes.[53]

FRT can also have chilling effects on free speech. FRT grants its users the ability to identify (or attempt to identify) people across spaces over time, making it a particularly powerful tool of surveillance. The potential for this tool to be used on people while they engage in activities protected by the First Amendment, including protesters or religious minorities attending a house of worship—may discourage people from engaging in these behaviors, for fear of being monitored. Without the ability to remain anonymous, it becomes harder to fully realize the right to First Amendment protected activities.[54]

Additionally, FRT may threaten equal protection because of the disparate impact it has on people of color.[55] Because Black and Brown neighborhoods are policed more heavily and harshly,[56] people from these communities are both more likely to be exposed to FRT, as well as more likely to be represented in arrest photos with which most FRT databases are built.[57] This means they are more likely to show up as a result as a "possible match" in an FRT search. On top of this, as mentioned previously, many FRT algorithms perform worse on people with darker skin.[58]

II. 2022: VIRGINIA'S PARALLEL FRT BILLS

In the 2022 session of the Virginia General Assembly, lawmakers allowed for the widespread and largely unregulated use of FRT by local law enforcement and campus police.[59] This change in the law saw a unique composition of bipartisan support and opposition, lending support to the phrase "politics makes strange bedfellows."

Prior to 2020, the issue of the use of FRT in Virginia by law enforcement and campus police had not come up for consideration or regulation in the

[52] Carpenter v. U.S., 138 S. Ct. 2206, 2223 (U.S. 2018).

[53] *See infra* Section III(A).

[54] *See generally* Clare Garvie, *Face Recognition and the Right to Stay Anonymous*, *in* CAMBRIDGE HANDBOOK OF INFO. TECH., LIFE SCI. AND HUM. RTS. (2022).

[55] Garvie, *supra* note 1, at 79.

[56] Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data*, 14 ANN. REV. OF LAW AND SOC. SCI. 293, 297 (2018).

[57] Garvie et al., *supra* note 5.

[58] Cook et al., *supra* note 3, at 1.

[59] VA. CODE §§ 15.2-1723.2, 23.1-815.1, 52-4.5.

General Assembly. FRT was similarly, and currently still is, unregulated by the federal government.[60] In 2020, Delegate Lashrecse Aird introduced House Joint Resolution 59.[61] This joint resolution directed the Joint Commission on Technology and Science to form a work group to study the proliferation and implementation of FRT and other artificial intelligence technology within the Commonwealth of Virginia.[62] A summary of the work group findings and recommendations was requested to be provided by the first day of the 2021 General Assembly session.[63] These requests for studies are regularly ordered by the General Assembly to convene stakeholders prior to proposing legislation.[64] This resolution was assigned to the subcommittee on Studies within the Committee on Rules. On January 29, 2020, this subcommittee recommended laying this resolution on the table by a vote of 6-0 and no workgroup was formed.[65]

The very next year, in the 2021 Session of the General Assembly, Delegate Aird introduced House Bill 2031,[66] which was commonly referred to as a "ban" on the use of FRT in Virginia. This bill received no opposition at any stage of the legislative process and was ultimately signed into law by Governor Ralph Northam during the Special Session on April 7, 2021.[67] This "ban" on the use of FRT by local law enforcement and campus police was codified in Virginia Code §§ 15.2-1723.2 and 23.1-815.1.[68]

These code sections prohibited the use of FRT by local law enforcement and campus police effective July 1, 2021, unless expressly authorized by the General Assembly.[69] However, the Virginia State Police (VSP) were not

[60] Lauren Feiner & Annie Palmer, *Rules Around Facial Recognition and Policing Remain Blurry*, CNBC (Jun. 12, 2021) https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html, But see, Blueprint for AI Bill of Rights, Office of Science and Technology, The White House, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[61] *HJ Res. 59 Facial Recognition and Artificial Intelligence Technology; Joint Com. on Science & Tech to Study.*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?201+sum+HJ59 (last visited Nov. 13, 2022).

[62] *Id.*

[63] *Id.*

[64] *S. 581 Correctional Facilities, Local and Regional; Fees Charged to Inmates*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+sum+SB581 (last visited Nov. 13, 2022). A similar work group was formed in Massachusetts to study the government's use of FRT. *See Final Report*: *Special Commission to Evaluate Government Use of Facial Recognition Technology in the Commonwealth*, FACIAL RECOGNITION COMM'N (Mar. 14, 2022), https://frcommissionma.com/.

[65] *HJ 59 Facial Recognition and Artificial Intelligence Technology; Joint Com. on Science & Tech to Study*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?201+vot+H2001V0028+HJ0059 (last visited Nov. 10, 2022).

[66] *HB 2031 Facial Recognition Technology; Authorization of use by Local Law-Enforcement Agencies, etc.,* VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+HB2031 (last visited Nov. 13, 2022).

[67] *Id.*

[68] H.D. 2031, 2021 Gen. Assemb. Reg. Sess. (Va. 2021).

[69] *Id.*

covered under this law and continued to use FRT without regulation from the General Assembly until 2022.[70] Additionally, the 2021 "ban" did not prohibit any local law enforcement agency from requesting the use of FRT through the VSP. In fact, in data provided by the VSP, of their 282 uses of FRT from 2018 through 2021, 105 were made at the request of local law enforcement.[71] Of those 282 uses, only 30 were by Virginia State Police themselves.[72] The remaining 147 uses were requests by other federal agencies or law enforcement agencies from other states.[73] VSP's own data show that the vast majority of cases where FRT was used were low-level offenses—the kinds of crimes most often captured on camera—not serious or violent crimes.[74]

Six months after this "ban" went into effect, two bills were introduced to permit the use of FRT by local law enforcement and campus police, despite those agencies' ability to use this technology through the VSP. House Bill 1339 (HB 1339) was introduced by Delegate Jay Leftwich, a Republican representing House of Delegates District 78, which includes parts of the city of Chesapeake in the Hampton Roads area.[75] Senate Bill 741 ("SB 741") was introduced by Senator Scott Surovell, a Democrat representing Senate District 36, which covers parts of Fairfax, Prince William and Stafford Counties in Northern Virginia.[76]

These bills, as initially introduced, were very similar; they each described what was meant by "facial recognition technology" and set out a list of criteria for lawful use of the technology as well as annual reporting requirements.[77] The following subsections include a discussion of each bill's movement through the legislative process, leading to the ultimate signing of a revised SB 741 by Governor Youngkin on April 27, 2022.[78]

A. HOUSE BILL 1339

HB 1339, as initially introduced, provided a definition of what facial

[70] *Id.*

[71] *See* Virginia State Police data (on file with the authors).

[72] *Id.*

[73] *Id.*

[74] *See What's Wrong with Public Video Surveillance*, ACLU (Mar. 2002), https://www.aclu.org/other/whats-wrong-public-video-surveillance; *see also*, Virginia State Police data (on file with the author) (showing that 116 of the 282 uses from 2018-2021 were for fraud incidents, 31 were for theft/larceny and 24 for homicide/manslaughter).

[75] *HB 1339 Facial Recognition Technology; Redefines, Local Law Enforcement and Campus Police to Utilize*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+sum+HB1339#:~:text=The%20bill%20directs%20the%20Virginia,Safety%20by%20November%201%2C%202025 (last visited Nov. 10, 2022).

[76] *SB 741 Facial Recognition Technology; Authorized Uses*, Va.'s Legis. Info. Sys., https://lis.virginia.gov/cgi-bin/legp604.exe?ses=221&typ=bil&val=sb741 (last visited Nov. 10, 2022).

[77] *Id.;* H.D 1339, 2022 Gen. Assemb., Reg. Sess. (Va. 2022).

[78] S. 737, 2022 Gen. Assemb., Reg. Sess. (Va. 2022).

recognition technology means and granted local law enforcement and campus police very broad authority to use FRT.[79] Several criteria were outlined for the usage of FRT for "criminal investigative and administrative investigative purposes."[80] The most significant criteria outlined were (1) that any FRT used must have "received an accuracy score of 98 percent or better for true positives across all demographic groups in the Facial Recognition Vendor Test" as evaluated by (NIST);[81] (2) that no match made by FRT can be probable cause for an arrest; and (3) matches made by FRT may be used for exculpatory evidence.[82] Furthermore, the initial bill mandated that the Department of State Police develop and publicly post a model policy for the use of FRT by January 1, 2023.[83] Lastly, the bill allowed local law enforcement agencies to develop their own policies, but required them to publicly post their policies prior to using the technology.[84] Record keeping and annual reporting were also required.[85]

This bill was referred to the Committee on Public Safety, a subcommittee of which recommended reporting the bill to the full committee by a vote of 6-2.[86] In that subcommittee, the patron, Delegate Leftwich, indicated that he viewed the ban from 2021 as a "timeout so that we could evaluate that practice and get it into a good format" and that he believed "this bill does exactly that."[87] Delegate Leftwich introduced an expanded version of the bill to the subcommittee and a lobbyist representing Clearview AI[88] provided public testimony at the subcommittee hearing.[89] This version allowed for fourteen "authorized uses" of FRT.[90] The patron also noted that the software pulls images from publicly available photos and pulls from a national database.[91] Subsection one of the authorized uses noted that FRT could be used to "identify an individual when there is a reasonable suspicion the individual has committed, is committing, or is planning to commit a crime."[92] This

[79] H.D. 1339, *supra* note 77.

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] *Id.* (The policy was released December 31, 2022 after all editing had been completed).

[84] *Id.*

[85] *Id.*

[86] *HB 1339 Facial Recognition Technology; Redefines, Local Law Enforcement and Campus Police to Utilize*, supra note 75 (recorded vote on H.D. 1339).

[87] *House Public Safety Subcomm. #2*, VA. HOUSE OF DELEGATES VIDEO STREAMING (Feb. 10, 2022), https://sg001-harmony.sliq.net/00304/Harmony/en/PowerBrowser/PowerBrowserV2/20221030/-1/14264 (advance video to 8:38:45-8:39:01).

[88] For more discussion of Clearview AI, *see infra* Section III(D).

[89] *House Public Safety Subcommittee #2*, *supra* note 87 (advance video to 8:58:00-8:58:50).

[90] H.D. 1339, *supra* note 77 (as amended by H. Comm. on Pub. Safety, Feb. 11, 2022).

[91] *House Public Safety Subcommittee #2*, *supra* note 87 (advance video to 8:41:43-8:42:03).

[92] H.D. 1339, *supra* note 77 (as amended by H. Comm. on Pub. Safety, Feb. 11, 2022).

definition is incredibly broad and could apply to someone who was planning to jaywalk, for instance. While jaywalking is an extreme example and likely almost impossible to detect, it illustrates that under the substitute, FRT could have been used in any way and for any alleged crime.[93]

The revised HB 1339 narrowly passed out of the Full Public Safety committee by a vote of 11-10.[94] On the floor of the House of Delegates on February 14, 2022, the patron, Delegate Leftwich, added additional amendments to the bill,[95] which included a sunset clause, a Class 3 misdemeanor penalty ($500 fine) for unauthorized use and termination for a second violation, and a provision for specific data collection, including the collection of demographic information. The bill passed out of the full House of Delegates by a vote of 71-29.[96] The bill then crossed over to the Senate for its review and vote.[97]

B. SENATE BILL 741

SB 741 broadly defined how FRT could be used "for investigating a specific criminal incident, or a specific citizen welfare situation."[98] Neither of these terms were defined and, much like HB 1339's initial draft, allowed for very broad use of FRT in almost any situation. The Senate bill also had the same NIST provisions regarding accuracy, and interestingly spelled out in fairly specific detail the type of training that the Department of State Police should outline in its model policy.[99] This bill was referred to the Senate Judiciary Committee on January 21, 2022.[100] This committee is typically where all bills are heard that create new crimes, amend existing crimes, or involve changes to policing practices or the use of technology, like body-worn

[93] The authorized uses included several additional applications, like identifying trafficking victims or deceased individuals, or helping to mitigate an imminent threat to public safety or national security, among many others. The subsequent discussion will focus on the use of FRT for criminal arrests and prosecution, as this is the area most ripe for misuse and abuse.

[94] Public Safety Committee Voting Record on *HB 1339: Facial Recognition Technology; Redefines, Local Law Enforcement and Campus Police to Utilize*., VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+vot+H15V0044+HB1339 (last visited Nov. 10, 2022).

[95] *See (HB 1339) Amendment(s) Proposed by the House*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+amd+HB1339AH (last visited Nov. 10, 2022).

[96] House Voting Record on *HB 1339 Facial Recognition Technology; Redefines, Local Law Enforcement and Campus Police to Utilize.*, VA.'S LEGIS. INFO. SYS. https://lis.virginia.gov/cgi-bin/legp604.exe?221+vot+HV1021+HB1339 (last visited Nov. 10, 2022).

[97] While all of this tinkering with HB 1339 was happening, a parallel FRT bill was making its way through the Senate. While HB 1339 crossed over the Senate for consideration, the remainder of this section will be spent on Senate Bill 741, as this is the version that received the most attention and editing and ultimately became law on July 1, 2022.

[98] S. 741(B), 2022 Gen Assemb., Reg. Sess. (Va. 2022).

[99] S. 741(C), 2022 Gen. Assemb., Reg. Sess. (Va. 2022).

[100] *See SB 741 Facial Recognition Technology; Authorized Uses*, *supra* note 76.

cameras[101] or weapons.

On January 31, 2022, this bill was re-referred to the Committee on General Laws and Technology.[102] When it was heard in this committee, Major Christian Quinn of Fairfax testified that when he retired in 2021, the technology had been used in Fairfax and Northern Virginia more than 12,000 times with "no misidentifications, no negative outcomes."[103] The committee had a discussion about using this technology for surveillance or profiling and decided that the technology was for investigation only.[104] This bill passed out of subcommittee with a substitute[105] with twelve "yes" votes and one abstention.[106] SB 741 passed out of the full Senate on February 15, 2022, by a vote of 26-14.[107]

When SB 741 crossed over to the House of Delegates, like HB 1339, it was referred to the House Public Safety Committee.[108] The Senate bill then began to mirror HB 1339, by adding fourteen specific authorized uses for FRT, a sunset clause, a Class 3 misdemeanor penalty for misuse and collection of certain demographic information for annual reporting.[109] This substitute passed out of the full Public Safety subcommittee by a vote of 14-7.[110]

SB 741 then failed to pass out of the House of Delegates on March 3, 2022.[111] In a procedural move to keep the bill alive, the vote was reconsidered

[101] *See* e.g., *HB 1327 Local Law-Enforcement Agencies; Body-Worn Cameras*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?ses=161&typ=bil&val=HB1327 (last visited, Nov. 8, 2022); *SB 1052 Body-worn Camera; Release of Recordings, Penalty*, VA. LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?ses=191&typ=bil&val=SB1052 (last visited Nov. 8, 2022).

[102] *SB 741 Facial Recognition Technology; Authorized Uses*, *supra* note 76.

[103] *General Laws and Technology - SR 3 - 30 min. after adjournment*, VA. S. (Feb, 9, 2022), https://virginia-senate.granicus.com/MediaPlayer.php?view_id=3&clip_id=4947 (advance video 45:31).

[104] *Id.* (advance video to 58:41).

[105] S. 741, 2022 Gen. Assemb., Reg. Sess. (Va. 2022).

[106] Committee Vote Record on *SB 741 Facial Recognition Technology; Authorized Uses.*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+vot+S12V0086+SB07411/12022%20SESSIONSB741Facialrecognitiontechnology;authorizeduses.02/09/22%20%20Senate:%20Reported%20from%20General%20Laws%20and%20Technology%20with%20substitute%20(12-Y%200-N%201-A)YEAS--Barker,%20Ruff,%20Locke,%20Vogel,%20Ebbin,%20Dunnavant,%20Mason,%20Boysko,%20Stuart,%20Pillion,%20Bell,%20Kiggans--12.NAYS--0.ABSTENTIONS--Hashmi--1 (last visited Nov. 8, 2022).

[107] Senate Vote Record on *SB 741 Facial Recognition Technology; Authorized Uses,* VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+vot+SV0446SB0741+SB0741 (last visited Nov. 10, 2022).

[108] *SB 741 Facial Recognition Technology; Authorized Uses.*, *supra* note 76.

[109] S. 741, *supra* note 105.

[110] Public Safety Committee Voting Record on *SB 741 Facial Recognition Technology; Authorized Uses*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+vot+H15V0079+SB0741 (last visited Oct. 24, 2022).

[111] House Voting Record on *SB 741 Facial Recognition Technology; Authorized Uses*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+vot+HV1425+SB0741 (last visited Oct. 24, 2022).

and then passed by for the day for a vote on the next day.[112] One day became seven days, as more time was needed to get the votes to pass out of the House of Delegates.[113] Delegate Leftwich then made amendments to the bill that prohibited the VSP, local law enforcement, and campus police from using FRT to track movements of individuals in public spaces, and prohibited service providers from keeping a comparison image except as required for auditing.[114] These amendments also increased the penalty for a second or subsequent misuse to a Class 1 misdemeanor.[115] With these amendments, SB 741 passed the House of Delegates by a vote of 54-42.[116] Since amendments were made to the bill after it passed the Senate, SB 741 went back to the Senate for its approval of the amendments, which was obtained on March 10, 2022.[117]

The bill then went to Governor Glenn Youngkin for his review on April 11, 2022, where he made several minor recommendations.[118] These recommendations specified that the model policy promulgated by the VSP "administer protocols for handling requests for assistance in the use of facial recognition technology made to the Department by local law-enforcement agencies and campus police departments."[119] Prior to the enactment of this law, local and campus police could use VSP's FRT by requesting their assistance, so this change only emphasized that FRT was and still is available through a centralized, independent agency. Additionally, the Governor recommended that "[r]equirements for training facilitated through the Department [of State Police] be included as part of the model policy.[120] These recommendations were adopted by the General Assembly and the bill became law on July 1, 2022.[121]

[112] *SB 741 Facial Recognition Technology; Authorized Uses*, *supra* note 76.

[113] *Id.*

[114] *SB 741 Amendment(s) Proposed by the House*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+amd+SB741AH (last visited Nov. 10, 2022).

[115] *Id.*

[116] House Vote Record on *SB 741 Facial Recognition Technology; Authorized Uses*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+vot+HV1662+SB0741 (last visited Nov. 10, 2022).

[117] Senate Vote Record on *SB 741 Facial Recognition Technology; Authorized Uses*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+vot+SV1036SB0741+SB0741 (last visited Nov. 10, 2022).

[118] *SB 741 Facial Recognition Technology; Authorized Uses*, *supra* note 76.; *SB 741 Governor's Recommendation*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?221+amd+SB741AG (last visited Nov. 10, 2022).

[119] *SB 741 Governor's Recommendation*, *supra* note 118.

[120] *Id.*

[121] VA. CODE §§ 15.2-1723.2, 23.1-815.1, 52-4.5 (2022).

III. HOW VIRGINIA'S LAW FAILS TO ADDRESS THE UNIQUE RISKS OF FRT

The Virginia FRT law fails to acknowledge and address the many unique risks that come from law enforcement's use of this technology. While the legislative process for SB 741 to become law seems long and convoluted, the entire process took just over three months from ban to approval.[122] This rapid expansion of FRT certainly has implications for the privacy of Virginians and those suspected or charged with crimes in the Commonwealth.[123]

Currently, there are more questions than answers. A lot has been made of the fourteen "limited" authorized uses that the legislature approved.[124] However, these authorized uses cover anything from identification of a victim of potential human trafficking and mitigation of an imminent threat of terrorism to suspicion that someone stole a bag of potato chips.[125] The proponents of FRT in Virginia point to its successful uses and argue that FRT merely makes law enforcement's job more efficient.[126] In other words, they contend that if law enforcement had time to look through all of the photos within whatever database they chose, whether that be booking photos, driver's license photos, or all publicly available photos on the internet, they would arrive at the same conclusion as FRT.[127] The issue with that assertion lies in the flaws of FRT, the reliance on technology, and overall faith in an algorithm.[128]

A. NO WARRANT REQUIRED

Virginia's FRT does not require law enforcement to obtain a warrant or

[122] *SB 741 Facial Recognition Technology; Authorized Uses*, *supra* note 76.

[123] *See*, Stone, Gavin, Norfolk police look toward drone surveillance to add more 'eyes' downtown, The Virginian-Pilot (Sept. 2, 2022), https://www.pilotonline.com/news/crime/vp-nw-drones-downtown-norfolk-crime-20220902-ziidq2yuibfprezo5jkefwi3hq-story.html (noting concerns by a senior staff attorney at the Virginia chapter of the ACLU about the cross-indexing of drone footage with a facial recognition database).

[124] VA. CODE § 15.2-1723.2 (2022).

[125] *Id.*

[126] *See* Jake Parker, *Examples of Successful Use of Facial Recognition in Virginia*, SEC. INDUS. ASS'N (Mar. 15, 2022), https://www.securityindustry.org/2022/03/15/examples-of-successful-use-of-facial-recognition-in-virginia/ (Security Industry Association is a trade organization for global security solutions).

[127] *See id.* (Security Industry Association is highlighting the speed and effectiveness of FRT).

[128] *See supra* Section II.

court order before conducting a search using the technology.[129] As such, police officers can use this software without any kind of regulation or oversight from an independent body that could ensure that the technology is not being overused or misused. This leads to a complete lack of transparency in its usage by the government. The Virginia law states that a match made through the use of FRT "shall not be included in an affidavit to establish probable cause for purposes of issuance of a search warrant or an arrest warrant."[130] This means that, without required disclosure in criminal cases, it is likely that no one will ever know that FRT was used unless defense attorneys specifically ask in every case.

Much is made of FRT only being an "investigative tool"[131] that functions as the first step in the process to narrow down potential subjects, before a human steps in to narrow down the alleged matches and continue the investigation.[132] There are several problems with this viewpoint. First, just because FRT is prohibited in any search warrant affidavit or to establish probable cause for arrest does not mean that it is not being used. Second, the prohibition against its inclusion means that it is very likely that no one will know that FRT is being used and abused. Lastly, it creates a false sense of urgency for the use of FRT, by avoiding any legal or judicial oversight prior to its use.

While the U.S. Supreme Court has not addressed whether a FRT search is considered a search under the Fourth Amendment, there is legal precedent to suggest that it should be treated as such. The Fourth Amendment protects people from unreasonable searches when they have a subjective expectation of privacy that society recognizes as reasonable.[133] The U.S. Supreme Court has stated that the Fourth Amendment is designed to protect people, not

[129] Eliana Block, *VERIFY: New Virginia Law Lets Local, Campus Police Use Facial Recognition Technology. How Can They Use It?*, WUSA9, https://www.wusa9.com/article/news/verify/when-can-virginia-state-local-and-campus-police-use-facial-recognition-technology/65-d125aa62-6790-4fe8-80e6-1d8d1b0d74f8 (last updated July 12, 2022) (quoting content from @ACLUVA, TWITTER (July 1, 2022), https://twitter.com/ACLUVA/status/1542865191850971137?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctw-term%5E1542865191850971137%7Ctwgr%5E0db3f44444141f36b2c4d72c86439b17c6d81aff%7Ctw-con%5Es1_&ref_url=https%3A%2F%2Fwww.wusa9.com%2Farticle%2Fnews%2Fverify%2Fwhen-can-virginia-state-local-and-campus-police-use-facial-recognition-technology%2F65-d125aa62-6790-4fe8-80e6-1d8d1b0d74f8).

[130] VA. CODE § 15.2-1723.2(C) (2022); *see supra* Section III(B).

[131] *See supra* Section II(A); *see also* Hoan Ton-That, *What Clearview AI has Implemented to Ensure That Facial Recognition Technology is Used Responsibly*, CLEARVIEW AI (Apr. 21, 2022), https://www.clearview.ai/post/what-clearview-ai-has-implemented-to-ensure-that-facial-recognition-technology-is-used-responsibly.

[132] *See e.g.* Clearview AI's Law Enforcement Page, CLEARVIEW AI, https://www.clearview.ai/law-enforcement (last visited Nov. 9, 2022) (stating "[t]hese leads, when supported by other evidence, can help accurately and rapidly identify suspects, persons of interest, and victims to help solve and prevent crime").

[133] Katz v. United States, 389 U.S. 347, 361 (1967).

areas.[134] Even if what a person seeks to keep private is "accessible to the public," such as a phone booth conversation, it may still be constitutionally protected.[135] But in 1973, the Supreme Court stated that no one could reasonably have an expectation that their voice will remain private, much like their face.[136] Of course, no one could have foreseen how much technology would advance over the next forty years, and how people would respond to FRT.

As technology advances, people will naturally have shifting opinions on what privacy means to them. Great examples of a recent shift the Supreme Court has had to make in this regard is evident in *U.S. v. Knotts* and *U.S. v. Jones.* In both cases, law enforcement officers were tracking a suspect's vehicle.[137] In *Knotts*, law enforcement attached a radio transmitter to a container of chloroform they knew the suspect would be picking up.[138] The suspect drove around town with the container in his vehicle, and officers were able to track his movements.[139] The Court was faced with the question of whether this tracking amounted to a Fourth Amendment violation, and the Court ultimately found that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[140]

In *Jones*, law enforcement attached a tracker to the suspect's vehicle and followed his movements for a month.[141] When faced with the question of whether this violated Jones' Fourth Amendment rights, the Court ruled unanimously against the government on trespass grounds.[142] The Court iterated that "mere visual observation does not constitute a search,"[143] but held that when the officers attached a device to Jones's vehicle, they encroached on a protected area.[144]

While it is established that a police officer making a mere visual observation of an individual on a street is not considered a search under the Fourth Amendment, it is not established whether it is a Fourth Amendment search when a police officer uses a device that can identify who a person is and how they interact online. The answer to this turns on whether it is reasonable for

[134] *Id.* at 353.

[135] *See id.* at 351.

[136] United States v. Dionisio, 410 U.S. 1, 14 (1973).

[137] United States v. Knotts, 460 U.S. 276, 277 (1983); United States v. Jones, 565 U.S. 400, 402 (2012).

[138] Knotts, 460 U.S. 277.

[139] *Id.*

[140] *Id.* at 281.

[141] Jones, 565 U.S. 403.

[142] *Id.* at 410.

[143] *Id.* at 412.

[144] *Id.* at 410.

a person to assume that police officers can gather personal information about them from an image. The recent organization against FRT use suggests that it may not be reasonable.[145] FRT has transformed how people think about the information that can be derived from the image of a person's face, as FRT allows people to compare facial profiles as a biometric identifier, much like fingerprints. People's faces have now become a mechanism for gaining personal information about them.

Over the last couple of years, there have been several examples of people organizing to stop the use of this technology due to privacy concerns and the fact that their image is being used without their consent. In 2018, a group of residents successfully organized to prevent facial recognition cameras from being installed in their apartment building.[146] In 2020, it was revealed that some police departments used FRT at Black Lives Matter protests, which sparked an outcry and led to a series of bills being introduced to ban the use of the technology.[147] It also resulted in corporations like Amazon, IBM, and Microsoft announcing that they would no longer sell their facial recognition software to law enforcement agencies indefinitely, or until federal law addressed the matter.[148]

While the courts have not caught up to technological advances in this space, state legislation certainly can. Legislators could have built in safety mechanisms within the bill and forced law enforcement agencies to obtain a warrant before they run a FRT search. By failing to build in this safety mechanism, Virginia residents may be subjected to privacy violations.

B. BRADY, DISCOVERY, AND FRT

The lack of prior judicial authorization or oversight is very concerning for not only the privacy of all people in Virginia, but specifically those who are being investigated and charged with crimes as the result of secretive use of FRT. For them, the possibility of deprivation of liberty based on the use of FRT is very real.

[145] *See, e.g.,* Geoffrey A. Fowler, *Black Lives Matter Could Change Facial Recognition Forever – If Big Tech Doesn't Stand in the Way*, WASH. POST (June 12, 2020), https://www.washingtonpost.com/technology/2020/06/12/facial-recognition-ban/; Erin Durkin, *New York Tenants Fight as Landlords Embrace Facial Recognition Cameras*, GUARDIAN (May 30, 2019), https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex; Nicole Ozer et al., *Grassroots Activists Are Leading the Fight to Stop Face Recognition. It's Time for Congress to Step Up, Too.*, ACLU (June 17, 2021), https://www.aclu.org/news/privacy-technology/grassroots-activists-are-leading-the-fight-to-stop-face-recognition-its-time-for-congress-to-step-up-too.

[146] *See Ban Dangerous Facial Recognition Technology that Amplifies Racist Policing*, AMNESTY INT'L (Jan. 26, 2021), https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

[147] *See id.*

[148] Fowler*, supra* note 145.

In most criminal cases, the defense and Commonwealth engage in a process of discovery. This process is governed by Rule 3A:11 of the Rules of the Supreme Court of Virginia for all felonies in circuit court and all misdemeanors brought by indictment.[149] Rule 7C:5 governs discovery for misdemeanors that carry jail time and felonies at preliminary hearings.[150] These rules lay out several requirements for production of evidence by the Commonwealth to the defense, and vice versa.[151] Rule 3A:11 also provides a list of evidence that is discoverable, such as fingerprint analysis and scientific reports.[152]

The use and results of FRT should be encompassed in scientific reports, but it is not clear if courts will interpret the discovery rule to include FRT. Additionally, Rule 3A:11 only applies to felonies in circuit court or indicted misdemeanors.[153] This means that the use of FRT does not have to be disclosed prior to a preliminary hearing. Instead of disclosing the use of FRT, some police departments claim that an eyewitness identified the suspect, but in reality, the eyewitness makes the identification after the police show them photos from the facial recognition software.[154]

Commonwealth's Attorneys, as with all other prosecutors in the nation, are legally required to turn over what is commonly referred to as *Brady* material.[155] *Brady* established that the prosecutor must turn over any evidence favorable to the accused; this can be evidence that goes towards negating the defendant's guilt, reducing the defendant's potential sentence, or relating to the credibility of a witness.[156] The prosecutor has an affirmative duty to seek out this information within their own files, but also those of law enforcement and any other entity that is considered to be an arm of the state or Commonwealth.[157] If this evidence is not turned over, and the defense finds out about it, the defense is required to demonstrate that if such material evidence were disclosed and used effectively, it could affect the outcome of the trial or undermine confidence in the verdict.[158]

The eternal problem with disclosure of Brady information is the faith the

[149] Va. Sup. Ct. R. 3A:11.

[150] *Id.* at R. 7C:5.

[151] *Id.*

[152] *See supra* note 149.

[153] *See id.*

[154] *See* Khari Johnson, *The Hidden Role of Facial Recognition Tech in Many Arrests*, WIRED (Mar. 7, 2022), https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/.

[155] *See generally* Brady v. Maryland, 373 U.S. 83 (1963).

[156] Brady, 373 U.S. 87.

[157] *See* Brady, 373 U.S. 83; *see also Brady Material*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/brady_material (last updated June 2021).

[158] Kyles v. Whitley, 514 U.S. 419, 432, 434 (1995).

defense has to put in the Commonwealth to turn over this exculpatory information. In many jurisdictions throughout the Commonwealth, there is no open file discovery.[159] The use of FRT by law enforcement prior to arrest poses serious problems with how any Brady information generated from its use will be disclosed. As the statute is written, FRT cannot be used within an affidavit for a search or arrest warrant.[160] However, it is admissible as exculpatory evidence.[161] The problem becomes, how defense counsel, the client, or the Commonwealth's attorney would know that FRT had been used if it is not documented anywhere. Subsection E of the statute requires that local law enforcement "shall maintain records sufficient to facilitate discovery in criminal proceedings."[162] The statute, however, does not require law enforcement officials to automatically turn this information over, unlike in some jurisdictions, including New York, where prosecutors are required to automatically turn over discovery within a certain time period.[163] This means that in Virginia, criminal defense attorneys and their clients will be in the dark on whether this technology was used in their case.

Until FRT is rolled out and used by local law enforcement and campus police as permitted by Virginia Code § 15.2-1723.2, it is unknown what processes will be put in place to ensure compliance with Brady as it relates to the use of FRT, as well as compliance with the traditional discovery rules. The concern is that if FRT is being used prior to any arrest and is viewed as an investigative tool,[164] defense counsel may never know of its use. Likewise, if it is used to develop an initial investigative lead or set of subjects, that fact may never be known either because there is no required disclosure.[165] Facial recognition companies like Clearview AI point out that their technology "helps exonerate the innocent."[166] It is unknown how often FRT has been used to exonerate people, but again, it may also be impossible to know if exonerations ever result, given the secrecy surrounding the use of FRT within Virginia.

C. ACCURACY OF FRT AS APPLIED IN VIRGINIA

In order to use FRT in Virginia, the technology must have been evaluated

[159] *See* Kristi Wooten, *Virginia Criminal Discovery Rules: The End of an Era?*, WOOTEN L. GRP. (Apr. 7, 2022), https://wootenlg.com/resources/virginia-criminal-discovery-rules-the-end-of-an-era/.

[160] VA. CODE § 15.2-1723.2(C).

[161] *Id.*

[162] *Id.* at § 15.2-1723.2(E).

[163] Jill K. Sanders, *More Changes to New York's Discovery Laws*, PAPPALARDO & PAPPALARDO, LLP (May 3, 2022), https://pappalardolaw.com/2022/05/more-changes-ny-discovery-laws/.

[164] *See supra* Section II(A) for a discussion of FRT as an "investigative tool."

[165] *See generally* Va. Code § 15.2-1723.2 (2022) (providing no requirement that law enforcement disclose a lead or suspect was found using FRT).

[166] *See Legal Overview*, CLEARVIEW AI, https://www.clearview.ai/legal (last visited Oct. 24, 2022).

by NIST as part of their Face Recognition Vendor Test (FRVT).[167] FRVT produces reports evaluating the accuracy of different FRT vendors; the most recent version of this report was published on July 28, 2022.[168] To use FRT in Virginia, the vendor selected must have "(i) an accuracy score of at least 98 percent true positives within one or more datasets relevant to the application in a NIST Face Recognition Vendor Test report and (ii) minimal performance variations across all demographics associated with race, skin tone, ethnicity, or gender."[169] While this may appear to be a helpful provision that will prevent false positive matches, this provision does not tell the full story.

True positives are one way to measure accuracy, but false positives are also a very important data point to consider. A false positive means that the facial recognition software returns a result showing two people are the same person, when in fact they are two different individuals.[170] A false positive can lead to the police investigating an innocent person, or even making a false arrest or charge.[171]

The FRVT has an algorithm leaderboard which ranks all the vendors that it has tested using different gallery, probe photos, and gallery sizes.[172] Despite the statute's reliance on the 98% accuracy rating as evidence of the technology's reliability, this issue is much more complicated. To start, NIST does minimal operational testing in real life settings, like those where local law enforcement typically uses FRT.[173] It also performs some operational testing at the federal level with the Department of Homeland Security.[174] At the local and campus level, as is authorized in Virginia, law enforcement will likely be using probe photos[175] from either still photographs gathered through their own investigations or from surveillance cameras.

In order to understand the difference in accuracy ratings, it is helpful to look at an example. The top algorithm in the FRVT leaderboard is one made

[167] VA. CODE §15.2-1723.2(B) (2021).

[168] *Face Recognition Vendor Test (FRVT) Ongoing*, NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing (last visited Nov. 8, 2022); GROTHER ET AL., *supra* note 21.

[169] VA. CODE §15.2-1723.2(B) (2021).

[170] Charles H. Romine, Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy, NAT'L INST. OF STANDARDS AND TECH. (Jan. 15, 2020), https://www.nist.gov/speech-testimony/facial-recognition-technology-part-iii-ensuring-commercial-transparency-accuracy.

[171] *See supra* Section I(C) of this paper.

[172] NAT'L INST. OF STANDARDS AND TECH., FRVT 1:N IDENTIFICATION (last updated Oct. 21, 2022).

[173] Garvie, *supra* note 1, at 34.

[174] *See* U.S. DEP'T OF HOMELAND SEC., SCI. AND TECH. DIRECTORATE: 2021 BIOMETRIC TECHNOLOGY RALLY RESULTS WEBINAR (June 2, 2022); *see also Biometric Technology Rally*, U.S. DEP'T OF HOMELAND SEC. (Aug. 12, 2022), https://www.dhs.gov/science-and-technology/biometric-technology-rally.

[175] *See* Block*, supra* note 129; *see also supra* Section II(A) of this paper for a description of the FRT process.

by the company SenseTime.[176] When this algorithm was tested on a mugshot-to-mugshot comparison, where the enrollment database has 12 million photos, it achieved a false positive rate of 0.18%.[177] That same algorithm, when comparing "kiosk" (i.e. a low quality akin to a surveillance photo or an ATM camera photo) on a smaller database of similarly high quality photos achieves a false positive rate of 7.1%, even though it should be an easier task.[178] The algorithm with the lowest false positive error rate on the kiosk image test, one made by the company Paravision, still has a false positive rate of 6.1%.[179] That algorithm's mugshot-to-mugshot false positive rate is 0.45%.[180] These two examples show how widely varied the accuracy results can be depending on the gallery and probe images selected *and* the size of the database. Clearview's algorithm, in mugshot-to-mugshot comparisons, has a false positive rate of .89% and "visa" (i.e. high quality as required for government issued identifications) to "kiosk" is 10.7% false positive.[181] As mentioned in Section I, this accuracy rating as measured by NIST is only one component of how FRT should be looked at as an overall tool.[182] The Virginia law fails to acknowledge the role that humans play in the reliability of this technology.

Assuming accuracy can even be measured, numerous different factors that affect how accurate a particular algorithm is, many of which involve the interaction of humans, machines, and technology.[183] For example, the selection of the gallery of images that a law enforcement agency is going to use as its comparison group allows humans to interact and deselect certain images or types of faces to include.[184] If an agency uses a mugshot database, like the Virginia State Police do, then there is likely to be an overrepresentation of minorities within those pictures. However, the benefits of using a closed database (i.e., one that is limited by certain criteria, like arrest) is that it provides some checks and a basis for identity verification.

As demonstrated above, mugshot-to-mugshot comparisons provide the highest level of accuracy when the algorithms are tested by NIST.[185] This is because the algorithms, much like humans, are better at matching the faces of people who are alone, facing the camera and in a well-lit environment,

[176] NAT'L INST. OF STANDARDS AND TECH., *supra* note 172.

[177] *Id.*

[178] *Id.*

[179] *Id.*

[180] *Id.*

[181] NAT'L INST. OF STANDARDS AND TECH., DATASHEET: CLEARVIEWAI_000 (2021), https://pages.nist.gov/frvt/reportcards/1N/clearviewai_000.pdf.

[182] *See supra* Section II of this paper; *see also* Garvie, *supra* note 1, at 34.

[183] Garvie, *supra* note 1, at 34.

[184] *See supra* Section II(A) of this paper. For an additional in-depth discussion about the FRT search process, *see* Garvie, *supra* note 1, at 19-27; *see also supra* Section I(D) of this paper.

[185] NAT'L INST. OF STANDARDS AND TECH., *supra* note 172.

which is the definition of a mugshot or an identification photo like those used for driver's licenses or passports.[186] While the photos in the gallery may be clear, the probe photos generally are not and that is where problems can start.

Oftentimes, after the facial recognition system returns a match, a human will check the results, which may include multiple potential matches, ranging in various confidence scores.[187] The human analyst will look at the potential matches and pick out which ones seem viable to them. In New York and Detroit, the police department has policies in place that require two police officers to review the results from a facial recognition search.[188]

In 2015, a group of researchers tested the ability of trained passport officers who already used facial recognition in their work and untrained student participants to identify whether the facial recognition system returned an accurate match.[189] Trained passport officers and student participants were given one photo of the target and other photos of different candidates that the system returned as a possible match. They then had to determine whether the target photo was a match with any of the potential candidates. The researchers found that the trained passport officers chose the wrong image about half the time, which was not very different from the results of the untrained participants.[190]

The results of this study show that even if a human analyst is trained on FRT, they still may have a difficult time determining which photos are an accurate match. At a minimum, training can be provided to alleviate some false matches. However, Virginia's law fails to provide any guidelines toward the training that human analysts should receive to ensure accuracy. It is also unclear whether law enforcement agencies in Virginia have internal policies around human analyst training.

D. QUESTIONABLE VENDOR PRACTICES

Right now, it is unknown which algorithms or vendors local law enforcement or campus police are going to select. As long as they meet the requirements of the statute, each local law enforcement and campus police could use a different algorithm and vendor. This means that some could pick Clearview AI, which has an extremely large and problematic database of photos that

[186] William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does it Matter?*, CSIS (Apr. 14, 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.

[187] Johnson, *supra* note 154.

[188] *Id.*

[189] David White et al., *Error Rates in Users of Automatic Face Recognition Software*, PLOS ONE, (Oct. 14, 2015), at 1.

[190] *Id.* at 3-5.

have been taken from alleged public sources.[191] Others could pick algorithms that do not include a database of images and rather select their own database of mugshots, driver's license photos, or something else entirely. As a result, Virginia has the potential to become a patchwork of facial recognition algorithms.

In January 2020, Kashmir Hill from The New York Times wrote an expose on Clearview AI (Clearview), which was largely operating in the dark at the time.[192] Clearview AI is a facial recognition software company that allows people to upload a single photo of someone and in return, Clearview will show all other images of the person it has within its system.[193] The photos in Clearview's system are extracted from popular social media sites like Facebook, Twitter, Google, YouTube, and others.[194] At the time Hill reported on the company, Clearview's software was mostly being used by various law enforcement agencies and federal agencies, such as the Department of Homeland Security and the FBI.[195] After Hill's article was released, Clearview faced sharp criticism, with forty privacy and civil liberties organizations calling for the U.S. Privacy and Civil Liberties Oversight Board to recommend suspension of facial recognition systems in the federal government.[196] Clearview received cease and desist letters from Facebook, Google, YouTube, and Twitter.[197] And months later, Clearview faced numerous lawsuits.[198]

Notably, Clearview AI invested heavily in lobbyists for the 2022 General Assembly session in Virginia.[199] Since the writing of this article, Clearview

[191] *See infra* 194 for a discussion of Clearview AI.

[192] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It,* N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[193] *Id.*

[194] *Id.*

[195] *Id.*

[196] Letter from Alianza Nacional de Campesinas et al. on FRT Suspension to PCLOB Members, EPIC.ORG (Jan. 27. 2020), https://epic.org/wp-content/uploads/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf.

[197] Charlie Wood, *Facebook Has Sent a Cease-and-Desist Letter to Facial Recognition Startup Clearview AI for Scraping Billions of Photos,* INSIDER (Feb. 6, 2020), https://www.businessinsider.com/facebook-cease-desist-letter-facial-recognition-cleaview-ai-photo-scraping-2020-2.

[198] Adam Schwartz, *Victory! More Lawsuits Proceed Against Clearview's Face Surveillance*, ELEC. FRONTIER FOUND. (Feb. 15, 2022), https://www.eff.org/deeplinks/2022/02/victory-another-lawsuit-proceeds-against-clearviews-face-surveillance.

[199] Ned Oliver*, Virginia Lawmakers Move to End Ban on Police Facial Recognition Technology,* VA. MERCURY (Feb. 10, 2022), https://www.virginiamercury.com/2022/02/10/virginia-lawmakers-move-to-end-ban-on-police-facial-recognition-technology/*. See also Clearview AI*, VA. PUB. ACCESS PROJECT, https://www.vpap.org/lobbying/client/386680-clearview-ai/?disclosure_period=17 (last visited Nov. 10, 2022) (detailing Clearview AI's lobbying expenditures).

has continued to expand and market their technology to law enforcement.[200] Clearview continues to be very active in the state and federal law enforcement space.[201] It boasts "[t]he world's largest facial network" with more than 20 billion photos sourced from public images, including news media, mugshots and public social media.[202] Clearview CEO Hoan Ton-That stated in an interview with Drew Harwell from *The Washington Post* on April 27, 2022 that Clearview's technology was only used by government entities at that time.[203] Subsequently, there has been reporting that Clearview is expanding its sales to schools and other applications.[204]

Clearview has also been the subject of litigation by the American Civil Liberties Union in Illinois.[205] In the settlement, entered on May 4, 2022, Clearview was banned from selling its product to Illinois law enforcement for five years.[206] This litigation was taken up under the Illinois Biometric Information Privacy Act, a law that ensured residents of the state did not have their biometric identifiers captured without their consent.[207] Clearview is a unique product because it is not only selling the algorithm, but also a built-in

[200] *See* John Hewitt Jones, *Clearview AI CEO Says Company Focused on Winning Federal Agency Contracts This Yea*r, FEDSCOOP (Feb. 28, 2022), https://www.fedscoop.com/clearview-ai-hoan-ton-that-federal-contracts/ (discussing Clearview AI's plan to contract with federal government agencies throughout 2022).

[201] *See Accelerate Your Investigations: Supporting U.S. Law Enforcement Agencies*, CLEARVIEW AI, https://www.clearview.ai/law-enforcement (last visited Nov. 10, 2022) (highlighting Clearview AI's support of law enforcement agencies); *see also* Josh Axelrod, *Government Relies on Industry for Facial Recognition Technology*, BLOOMBERG L. (July 19, 2022), https://news.bloomberglaw.com/business-and-practice/government-relies-on-industry-for-facial-recognition-technology (discussing the government's continued willingness to contract with private sector facial recognition technology companies, including Clearview AI). *But see* Press Release, Ed Markey U.S. Senator for Mass., Senators Markey & Merkley and Reps. Jayapal & Pressley Urge Federal Agencies to End Use of Clearview AI Facial Recognition Technology (Feb. 9, 2022), https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal_pressley-urge-federal-agencies-to-end-use-of-clearview-ai-facial-recognition-technology (discussing letters sent by elected officials voicing serious concerns about facial recognition technology's "ability to eliminate public anonymity" and its "unique threats to Black communities, communities of color, and immigrant communities").

[202] *Accelerate Your Investigations: Supporting U.S. Law Enforcement Agencies*, *supra* note 201.

[203] Washington Post, *Clearview AI CEO Hoan Ton-That on Facial Recognition Technology*, YOUTUBE (Apr. 27, 2022), https://www.youtube.com/watch?v=0fxD39cvKXQ (advance video to 9:34).

[204] Paresh Dave, *Clearview AI's Facial Recognition Tool Coming to Apps, Schools*, U.S. NEWS & WORLD REP. (May 24, 2022), https://www.usnews.com/news/technology/articles/2022-05-24/clearview-ais-facial-recognition-tool-coming-to-apps-schools, and see, Hill, Kashmir, Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands, N.Y. Times https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html (Sept. 18, 2022).

[205] *In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois Biometric Privacy Law,* ACLU (May 9, 2022), https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois.

[206] Settlement Agreement & Release at 2, ACLU v. Clearview AI, Inc., No. 20 CH 4353 (Ill. Cir. Ct. May 4, 2022), https://www.aclu.org/sites/default/files/field_document/exhibit_2_signed_settlement_agreement.pdf.

[207] *Id.*

database of images collected from public spaces.[208] All other FRT companies only sell an algorithm, and the agency that purchases the algorithm selects whatever image database they want to use the algorithm against.[209] For example, a government could select its own, non-public mugshot database or its driver's license database. The Virginia law, while attempting to control the accuracy of the vendor selected, does not account for the controversial, and maybe illegal, practices used by some vendors.

E. VIRGINIA'S FRT LAW FAILS TO PREVENT HISTORICAL TRACKING

Finally, the Virginia law prohibits real time tracking of people in public spaces.[210] If one assumes that this type of tracking is not happening, then the argument against prior judicial authorization fails, because there is no scenario that is so urgent that a review of past photographs cannot be vetted prior to the use of FRT. Additionally, almost all of the authorized uses defined in Virginia law, along with the Virginia FRT success stories,[211] relate to non-emergency situations where a search or arrest warrant could have been authorized.[212] In order to curb police misuse and abuse and to foster transparency, the General Assembly could have started by authorizing FRT to aid in the identification of a deceased individual[213] or help identify a victim of human trafficking.[214] This approach would have been prudent, as the implications of the widespread use of FRT by law enforcement are unknown (and perhaps unknowable), but this approach would also balance public safety, privacy and due process. In its current form, the provision does prohibit, for example, law enforcement using FRT at a protest to identify someone at that moment.[215] While this is a good step, the law fails to acknowledge and address historical tracking. FRT can result in historical tracking, as it can allow

[208] *See* Drew Harwell, *Facial Recognition Firm Clearview AI Tells Investors It's Seeking Massive Expansion Beyond Law Enforcement*, WASH. POST (Feb. 16, 2022), https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/ (detailing Clearview AI's CEO's statements regarding how Clearview collects and stores images).

[209] RankOne is the algorithm used by the VSP and its algorithm is used on the VSP database of mugshots. Nicol Turner Lee & Caitlin Chin, *Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*, THE BROOKINGS INSTIT. (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/; *see also supra* Section II.

[210] VA. CODE § 15.2-1723.2(C) (2022); *but see* Ned Oliver, *Virginia Police Routinely Use Secret GPS Pings to Track People's Cell Phones,* VA. MERCURY (Apr. 6, 2022), https://www.virginiamercury.com/2022/04/06/virginia-police-routinely-use-secret-gps-pings-to-track-peoples-cell-phones/#:~:text=Real%2Dtime%20location%20warrants%20in,on%20behalf%20of%20law%20enforcemen (demonstrating that, despite the above Code of Virginia provisions, Virginia police have in fact used real time tracking on Virginia citizens).

[211] Parker*, supra* note 126.

[212] VA. CODE § 15.2-1723.2(A)(vii) (2022); *see also id.*

[213] VA. CODE § 15.2-1723.2(A)(vii) (2022).

[214] *Id.* at § 15.2-1723.2(A)(iv).

[215] *Id.* at § 15.2-1723.2(C).

police officers to track a person for years through their online presence and thereby create a timeline of events.[216] Police officers could also use this software to run an image of a person against surveillance camera footage, using the results to retrace a person's movements.

In the case *Carpenter v. United States*, the Supreme Court addressed the issue of historical tracking in regard to cell site location information (CSLI).[217] The government obtained cell site location records from Carpenter's wireless carrier that showed the location of Carpenter's phone whenever he made an outgoing call or received an incoming call for a period of 127 days.[218] The Court stated that because people take their phones with them everywhere, allowing the government to track people's location through their phones gives the government "near perfect surveillance, as if it had attached an ankle monitor to the phone's user" and allows them to "travel back in time to retrace a person's whereabouts."[219] Accordingly, the Court found that obtaining CSLI is a search that requires Fourth Amendment protections.[220]

FRT strikes right at the heart of the Court's ruling in *Carpenter*, as this software can allow law enforcement to travel back in time and track a person's movements. Virginia's FRT law has failed to account for this possibility and ban the use of historical tracking.

F. VIRGINIA'S FRT LAW ALLOWS FOR OVERBROAD USE

Many within the Virginia General Assembly made the point that FRT is already out there and being used, so the legislature might as well regulate it. However, their attempts to regulate FRT through this legislation fail for many reasons. First, as previously noted, the VSP were already using FRT and not subject to the ban.[221] Additionally, the VSP was facilitating the use of FRT for local law enforcement by request.[222] With the limited information we have about best practices for FRT use, other states and advocates have recommended centralizing FRT use to one agency as the best way to foster double-blind review and transparency.[223] This way, the officer who is running the

[216] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018); *see also* Dallas Hill et al. *Police Use of Facial Recognition Technology: The Potential for Engaging the Public Through Co-Constructed Policy Making*, 24 INT'L J. POLICE SCI. & MGMT. 325, 326-27 (2022).

[217] Carpenter, 138 S. Ct. 2211.

[218] *Id.* at 2209, 2212.

[219] *Id.* at 2218.

[220] *Id.* at 2222.

[221] Virginia State Police Data (noting that these technologies had been used by VSP as early as 2019) (on file with authors).

[222] *Id.* (noting that the originating agency in many Virginia cases was local law enforcement agencies) (on file with authors).

[223] *Final Report*: *Special Commission to Evaluate Government Use of Facial Recognition Technology in the Commonwealth, supra* note 64, at 27–28, 32 n.71.

FRT is not the officer who is also investigating.[224]

By their own account, the VSP were engaging in these practices and there was nothing stopping them from continuing to facilitate the use of FRT through their centralized agency.[225] With the July 2022 change, each local law enforcement agency is permitted to use and purchase their own FRT software and the only limitations are that they comply with the VSP model policy.[226] The statute directs the VSP to develop a policy that includes training requirements facilitated through VSP, "including the nature and frequency of specialized training required for an individual to be authorized by a law-enforcement agency to utilize facial recognition technology as authorized by this section."[227] Per statute, the model policy must also include "procedures for the confirmation of any initial findings generated by facial recognition technology by a secondary examiner."[228] Another point of concern is that the statute only requires departments to report their FRT use once a year, on April 1.[229] At the time this article was written, the model policy was not available, so time will only tell how this directive is interpreted and implemented.[230]

The Virginia FRT law provides a long array of circumstances where law enforcement can use FRT, which not only includes its use to identify people who may have committed a crime, but also allows its use to identify victims and potential witnesses.[231] By running searches on victims and potential witnesses, law enforcement will force people to have contact with police when they have no legal obligation. Witnesses and victims often decide not to report crimes because they fear retaliation and may choose to speak to counselors and organizations first for guidance.[232] By forcing people to come

[224] *See* Garvie, *supra* note 1, at 12 (asserting that face recognition is only a lead for investigation, but requires further investigation for probable cause); *see also* Giannelli, *supra* note 37, at 248 (noting that forensic scientists can become biased and more partisan when working with law enforcement); *see also* FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS, *supra* note 26, at 10 (discussing several types of bias that can occur, including cognitive bias, confirmation bias, and contextual bias).

[225] Virginia State Police Data (noting several instances of VSP's use of FRT) (on file with authors).

[226] VA. CODE § 15.2-1723.2 (2022).

[227] *Id.* at § 52-4.5(C)(1).

[228] *Id.* at § 52-4.5(C)(3).

[229] *Id.* at §§ 15.2-1723.2(F), 23.1-815.1(F), 52-4.5(F) (2022).

[230] The State Model Facial Recognition Technology Policy was released on December 31, 2022 after the final substantive edits were made to this article, as such it is not analyzed within this article. Per VA. CODE ANN. § 15.2-1723.2(D), local and campus law enforcement are now permitted to use FRT as long as they either adopt this model policy or develop their own policy within 90 days that meets or exceeds the standards within the VSP model policy.

[231] *Id.* at § 15.2-1723.2(A) (2022).

[232] *See Why Do So Many Crimes Go By Unreported In The States?*, NYU DISPATCH, (Aug. 31, 2018), https://wp.nyu.edu/dispatch/2018/08/31/why-do-so-many-crimes-go-by-unreported-in-the-states/ (describing that sexual assault victims are often censured or criticized when they decide to file reports, which ultimately deters other victims from coming forward. A clinical psychologist shared that many of her patients, as sexual assault victims, faced mistreatment from officers when filing reports).

forward before they have set up protections for themselves, law enforcement could put people at risk.

Many of these categories leave too much room for discretion on the part of law enforcement. Will police officers consider a person in the general vicinity of a crime a potential witness and run a facial recognition search on them? What about a person who does not reveal their identity to police officers? Will a police officer label them as someone who is "unable to identify himself?" The failure to place limitations on officer discretion will lead to the overuse of this technology in situations where it may be unwarranted.

CONCLUSION

Virginia's current FRT law does not adequately address the unique risks the technology poses. In failing to account for these unique risks, the law allows police to use FRT in a generally unregulated manner, and in ways that can harm privacy, free speech, due process, and other civil rights and liberties.