Government Use of Technology in Surveillance

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Matthew T. Beyer

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Dr. Kent A. Wayland, Department of Engineering and Society

Research Question & Significance:

How far can governmental powers ethically extend their use of facial recognition technology for surveillance and law enforcement purposes?

Advances in technology have led to amazing socioeconomic phenomena, but have also allowed for radicalization, terrorism, and the ability to steal from millions at the press of a button. As a result, law enforcement agencies across the globe have been scrambling to modernize and develop competing cutting-edge technology. Unfortunately, as new technologies arise, they are often put to use before their implications are fully understood and before legislation is enacted to regulate their ethical use. A particularly promising yet ethically concerning technology for law enforcement is facial recognition technology. As the Virginia General Assembly is passing laws that restrict yet enable police use of facial recognition technology, social activism groups are skeptical that the technology will be used properly, as its inherent technological flaws open the door to discrimination. The purpose of my research is to analyze the actants and social groups involved in the argument over Virginia law and provide insight into their positions on how facial recognition can be regulated for ethical use by the government to efficiently enforce rule of law while ensuring that said technologies are not used to oppress, endanger, or infringe upon the rights of civilians, but rather protect them.

Background:

If you have ever used autocorrect, unlocked your phone with your face, or talked to a virtual assistant on a website, you have interacted with artificial intelligence. Artificial intelligence "deals with all aspects of mimicking cognitive functions for real-world problem solving and building systems that learn and think like people" (Holzinger, 2019). This is often personified by the development of computer programs which can learn to classify and identify

things based on provided datasets and discover correlations that humans otherwise would not draw. This technology has a myriad of uses in the technical world, and can be found in use by many companies across the globe. While artificial intelligence can be used for good, its reduction of human beings to data points opens the door to oppression and misclassification, as context and social phenomena are often neglected in analysis of human behavior. This neglect has a specifically concerning impact on a specific branch of artificial intelligence that focuses on a person's physical appearance: facial recognition technology.

Facial recognition technology is when programs "(create) a 'template' of (a) target's facial image and compare the template to photographs of preexisting images" from a database with the goal of determining the target's identity (Andrejevic, 2020). This technology can be used for all kinds of purposes, ranging from employers tracking who is at work to advertisers targeting ads and governments using facial recognition to identify threats. While a Pew Research Center study found that a slight majority of American adults seem to trust the government using facial recognition, it seems that this may be in error, as a 2020 study by Lynch argued that facial recognition technology poses significant risks to civil liberties, including by disproportionately affecting people of color, since the technology is not as accurate at identifying women and people of color as it is at identifying white men (Smith,2019; Lynch, 2020). A deeper look into how the technology is used may help us understand its applications and its flaws.

Uses of Facial Recognition Technology in Law Enforcement:

Facial recognition technology uses algorithms to analyze and compare a person's facial features from an image or video with a database of stored images. Facial features that are analyzed can include the distance between the eyes, the shape of the nose, the contours of the

face, and more (Sclaroff, 2018). Even if you are unaware of any reason your face would be in a database, it is likely that law enforcement databases contain stored images of your face matched to your identification information. The Georgetown Law Center on Privacy and Technology published a 2016 report that found that more than half of American adults are in law enforcement facial recognition databases. The FBI has access to vast libraries of photos of Americans, many of which are acquired via social media (U.S. Government Accountability Office, 2021). Additionally, at least 26 states allow law enforcement to search for facial recognition matches in driver's license photographs and databases (Bedoya et al., 2016). The depth of these law enforcement databases is massive, but what do they use all of this data for?

The Georgetown Law Center report highlighted four common uses of facial recognition technology for law enforcement. First, they highlighted "Stop and Identify" uses, which include when an officer encounters someone who is unable to identify themselves or refuses to do so. The officer takes a picture of the person, and when uploaded, the system quickly outputs the identity of the person if it is known. While it varies state to state over if a person is required to identify themselves, this technology can be especially useful if the person is mentally incapacitated. An assumed use of this technology would be for if someone with Alzheimer's disease were to get lost and confused, the officer could use facial recognition to identify them and get them back to their home safely (Bedoya et al., 2016).

The next highlighted use of this technology is "Arrest and Identify" uses, wherein a person is arrested, and their mugshot is run through the database to identify them. Once this mugshot is entered in the database, the police may submit it to the FBI for further screening. The third listed use of facial recognition technology is "Investigate and Identify," which is when photos or videos of a suspect for a crime are submitted to the database for suspect identification.

Finally, the Georgetown Law Center also details “Real-time Video Surveillance,” wherein a “hot list” of individuals that police are looking for is submitted to a program which monitors live video feeds from many security cameras, alerting officers if one is identified. This technology can also be employed after the fact with archival video (Bedoya et al., 2016). The legality of this use is in question across many states, however some police departments are fervent in their support for its use in cases involving kidnapping and abduction, as both victims and suspects can be identified quickly in cases that often turn very dangerous after only a short period of time.

Despite the intended uses of the technology, its failure to correctly identify women and people of color, noted by Lynch’s 2020 article, adds an inherent racial and sex-based disparity in its function. This disparity has resulted in minority groups having special interests in the means of development and regulation of facial recognition—use of a flawed technology could result in false-positive identification of ordinary citizens as criminals and turn somebody’s life upside-down. When the public sees that the power they vested in the government to protect them may be used to harm them, it becomes their responsibility to elect or lobby leaders that will enact legislation that regulates such power. While we do not yet have substantial federal regulation of facial recognition technology in the United States, some state governments are starting to attempt to introduce legislation governing yet allowing its use by law enforcement.

State-Level Legislation in Virginia:

The Virginia House of Delegates passed a bill on February 15th, 2022 with the goal of redefining facial recognition technology and providing criteria to local law enforcement for lawful use of the technology (Virginia General Assembly, 2019). When this bill passed, it was sent to the Virginia Senate as Senate Bill 741 (SB-741), before finally being passed into law on

April 27th, 2022 by a vote of 50 in favor to 46 in opposition and signage by the Governor (Virginia General Assembly, 2021). The bill's official summary, in its final form, states the following (directly quoted from FastDemocracy, 2022)

A) The bill authorizes local law-enforcement agencies, campus police departments, and the Department of State Police to use facial recognition technology (FRT) for certain authorized uses.
B) The bill requires that the FRT in use be evaluated by the National Institute of Standards and Technology and have an accuracy score of at least 98 percent true positives across all demographic groups.
C) The bill requires the development of a Department of State Police model policy for use of FRT and that all localities must adopt the model policy or create their own which meets or exceeds the standards set by the Department of State Police model.
D) The bill requires local law-enforcement, campus police departments, and the Department of State Police to publish an annual report the public regarding the agency's use of FRT.
E) The bill clarifies that any match made through facial recognition technology shall not be used in an affidavit to establish probable cause for the purposes of a search or arrest warrant.
F) The bill states that any FRT operator who violates department policy for the use of FRT is guilty of a Class 3 misdemeanor for a first offense and a Class 1 misdemeanor for a subsequent offense.

While this bill is currently Virginia law, several lobbyist groups, including the Virginia branch of the American Civil Liberties Union, have loudly voiced their opposition to its signage.

Other groups, such as Bedford County Sherriff Michael W. Miller, have been in support of the bill, even writing to Virginia Governor Glenn Youngkin to attest in favor of its signage.

Methods:

Direct evidence was collected on both sides of the debate around the passage of SB-741. Sherriff Miller's letter argued in favor of the use of facial recognition technology for his police force on the grounds that in the event of a time-critical criminal investigation, such as a child abduction, time is of the essence, so utilizing the real-time video surveillance application of the technology could help save lives. Miller also acknowledged that he believed the provisions outlined in the potential bill would effectively counteract unintended negative consequences of the technology's imperfections. Not all sources would agree on this matter.

Among other sources, Powers et al.'s 2023 article *From Ban to Approval: What Virginia's Facial Recognition Technology Law Gets Wrong* was analyzed to gain an overall sense of the bill's opposition. The purpose of the article was to argue that the bill did not do enough to counteract the technology's bias, mainly arguing that since the bill did not require a warrant for use of the technology, law enforcement agents could use it in inappropriate scenarios. The article also acknowledged that while the bill did prohibit real-time tracking of a known individual in public places, it did not prohibit tracking after the fact, allowing government to essentially monitor a citizen's location without a warrant as soon as they leave.

Further evidence was gathered in opposition to the bill, primarily in the form of a letter from the ACLU of Virginia to the Virginia House of Delegates and Senate. The letter opposed the signage of SB-741 on the grounds that facial recognition technology has been used inaccurately and has resulted in the false criminal accusation of an African-American man in

Detroit, Michigan based off of a false-positive facial recognition result. This accusation led him to lose his job, even though he was found innocent, causing many groups to oppose the use of the technology.

After collecting arguments for and against SB-741, general objective information about the bill was found on several bill-tracking websites, including but not limited to Virginia's Legislative Information System. To generate results, concerns of each side were compared to actual provisions of the bill under each application scenario discussed by the Georgetown Law Center report to see how public concerns are addressed by the bill under each prospective use.

Results:

Stop and Identify Use of FRT

The "stop and identify" use of facial recognition technology is enacted when an officer comes across a civilian who is unable to or refuses to identify themselves. While the scenario in which a civilian in a mentally impaired state is identified and returned to their family is considered a public welfare situation and not controversial, the scenario where scenario wherein an officer identifies a subject who refuses to share their identity is. Under Virginia law, a citizen is required to identify themselves only when lawfully detained, which requires ample probable cause from the law-enforcement officer (Virginia Code § 19.2-74, 2023). If the citizen is not detained, they are able to exercise their right to remain silent. In scenarios where an officer identifies a citizen who is either not detained or unlawfully detained using facial recognition technology, this is problematic, because the rights of the citizen are being compromised by the availability of the technology. While this seems to be a clear-cut scenario wherein facial

recognition technology should not be allowed, in practice, citizens may be unaware of their rights and officers may choose to violate them.

To mitigate the costs of this contingency, SB-741 states in the above summary section E that no match made through FRT can be used to establish probable cause, disallowing an unlawful identification from resulting in the citizen being arrested or searched. This section is the most broadly impactful in terms of preventing overreach with the technology, and does the most to practically limit any negative results of unintended discrimination through technological bias. Even if law enforcement officers use the technology in a wrongful "stop and identify," manner there will be no legal ground for an officer to take action against the civilian.

Arrest and Identify Use of FRT

The "arrest and identify" application of facial recognition technology comes into play when a mugshot of an arrested person is run through the system to compare to known people. In this application, the technology's faults do allow the possibility that an innocent person falsely has their identity attributed to a criminal, but with biometrics such as fingerprints and circumstantial alibis existing and necessary to confirm an identity, it is extremely unlikely that this false-positive scenario would play out without being resolved as a mere system error.

Still, another way that SB-741 attempts to counteract these issues is by requiring a 98% true positive test rate across all demographics. While this is not perfect by any means, the clause that ensures all demographics are equally reliably covered by the technology should eliminate some of the potential for discrimination. Furthermore, this investigative process is already conducted by police who comb through thousands of images in the system by hand until they can find a match. The use of the technology in arrest and identify cases would only serve to make

law enforcement more efficient, saving officers hours of work, while still needing human confirmation after a possible match is identified.

Investigate and Identify Use of FRT

The "investigate and identify" use of facial recognition technology is when visual evidence such as CCTV footage of a suspect, victim, or witness is run through the facial recognition database to get a lead on an important actor in a criminal investigation. This use is one which is highly susceptible to false-positives, as photographic or video evidence is often grainy or unclear. This specific use is also the use which caused false accusations being levied towards Robert Williams: the African-American resident of Detroit who the ACLU noted had his reputation damaged by a false-positive facial recognition result.

The Virginia law's provision that facial recognition technology cannot be used to establish probably cause for an arrest or a search warrant should reduce the practical impact of this use of the technology. Still, as seen with Robert Williams, even an accusation without probable cause to arrest can still cause serious damage to an innocent person's reputation. Provision C of the above summary states that any police entity that wishes to use facial recognition technology should have a use policy which is at minimum as strict as the model policy suggested by the Department of State Police. While this should help minimize the occurrence of these false-positives by restricting the use to only serious scenarios (potentially only targeting violent crime as opposed to lesser crimes such as petty theft), there is no way of knowing how serious the downstream effects of these false-positives could be. Furthermore, focus on more serious crimes restricts usage scenarios, but does not curtail the reputation damage that can still occur from a false-positive accusation.

Real-Time Surveillance Use of FRT

The "real-time surveillance" application of facial recognition technology is when a list of individuals is constantly compared to video feed from a collection of cameras. When these individuals are identified, local law enforcement is notified of their location. As Sheriff Miller insists, this should be most useful application of the technology when searching for a missing person or in the event of a kidnapping. However, SB-741 explicitly bans "real-time tracking of a known person's movements in public spaces" (Parker, 2022). While this provision is intended to steer the use of technology away from surveillance, critics argue that it is not enough. While the bill bans "real-time tracking," it does not ban tracking of an individual after the fact, so a shortly delayed surveillance system could be considered legally ambiguous. Curiously, this provision appears to appease neither those in favor of the "real-time surveillance" use of the technology nor those critical of it.

Discussion:

I have gathered evidence involving the concerns of groups both in favor and against the implementation of SB-741 and have evaluated the implications of the specific provisions of the law with regards to these concerns based on the most common uses of facial recognition technology. In "arrest and identify" cases, I do not believe that the technology's inherent flaws introduce any extraneous bias which could harm minority groups, because it only streamlines redundant identification processes which already occur during such uses. SB-741 attempts to address all potentially discriminatory uses of the technology by having provision E limit the technology as only supplemental evidence, never capable of justifying an arrest or search warrant on its own. While this seems to effectively address potential discriminatory issues in "stop and identify" uses of the technology, it does not do enough to mitigate the risk of serious damage to

reputation during “investigate and identify” scenarios. Furthermore, the bill’s ban on “real-time surveillance” use satisfies neither those opposed to the technology nor those in favor of it, since it fails to address after-the-fact surveillance while significantly hindering real-time surveillance which could greatly impact time-sensitive kidnapping investigations.

Conclusion:

Groups in favor of Virginia’s SB-741 allowing law enforcement to use facial recognition technology are largely in favor due to the potential impact the technology can have on making law enforcement more efficient and effective when provided limited evidence. Those who are against the bill generally cite the poor accuracy of the technology at identifying those in minority groups, thus exposing them to unnecessary and disproportionate risk of false-positive identification and subsequent ramifications. While SB-741 effectively mitigates risk of discrimination in “stop and identify” and “arrest and identify” uses of the technology, it does not do enough to curtail risk of serious reputation damage from “investigate and identify” scenarios. Furthermore, SB-741 fails at providing law enforcement the tools they need in “real-time surveillance” situations as well as at protecting from an “after-the-fact” surveillance state.

Facial recognition technology can be a valuable tool to law enforcement by increasing their efficiency in investigations, however the technology’s inherent bias poses a subsequent risk to civil liberties which are only partially protected by Virginia’s new law. As facial recognition technology becomes more commonplace across the commonwealth, other jurisdictions should take note of the successes and failures of Virginia’s legislation as they plan their own regulation of the technology.

References

ACLU. (n.d.). Face recognition technology. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology

ACLU of Virginia. (March 3, 2022). [ACLU of Virginia writes to the Virginia House of Delegates and the Virginia Senate to oppose Senate Bill 741 and House Bill 1339.] Retrieved from https://www.acluva.org/en/press-releases/aclu-va-sends-joint-letter-opposing-facial-recognition-technology

Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology in schools: Critical questions and concerns. Learning, Media and Technology, 45(2), 115-128. https://doi.org/10.1080/17439884.2020.1686014

Bedoya, A. M., Frankle, J., & Garvie, C.. (2016). The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy and Technology. https://www.perpetuallineup.org/

FastDemocracy. (2022). Virginia House Bill 2244. https://fastdemocracy.com/bill-search/va/2022/bills/VAB00022441/

Holzinger, A., Langs, G., Denk, H., Zatloukal, K., & Müller, H. (2019). Causability and explainability of artificial intelligence in medicine. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9(4), e1312.

Lynch, J. (2020). Face Off: Law Enforcement Use of Face Recognition Technology. Electronic Frontier Foundation. Available at SSRN: https://ssrn.com/abstract=3909038

Miller, Michael W. (April 7, 2022). [Sheriff Miller of Bedford County voices support of Virginia SB 741 to VA Governor Glenn Youngkin.] Retrieved from https://vasheriff.org/2022/04/10/letter-to-governor-youngkin-support-sb-741-to-allow-law-enforcement-agencies-in-the-commonwealth-of-virginia-to-utilize-facial-recognition-technology/

Parker, J. (2022). Virginia's New Rules for Facial Recognition and What They Mean. Security Industry Association. Retrieved from https://www.securityindustry.org/2022/03/15/virginias-new-rules-for-facial-recognition-and-what-they-mean

Powers, A., Simon, K., & Spivack, J. (2023). From Ban to Approval: What Virginia's Facial Recognition Technology Law Gets Wrong. Richmond Public Interest Law Review, 26(1), 155-184.

Sclaroff, S., & Zhang, H. (2018). A survey of facial recognition: From traditional techniques to deep learning. Proceedings of the IEEE, 106(12), 1969-1996.

Smith, A. (2019). More than half of US adults trust law enforcement to use facial recognition responsibly. Pew Research Center, 5.

U.S. Government Accountability Office. (2021). Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks. https://www.gao.gov/products/gao-21-579

Virginia Code § 19.2-74 (2023). Retrieved from https://law.lis.virginia.gov/vacode/title19.2/chapter5/section19.2-74/

Virginia General Assembly. (2019). House Bill 1339. https://lis.virginia.gov/cgi-bin/legp604.exe?ses=191&typ=bil&val=hb1339

Virginia General Assembly. (2021). SB 741 Voting Record - House of Delegates. https://lis.virginia.gov/cgi-bin/legp604.exe?221+vot+HV1832+SB0741