King County

Metropolitan King County Council
Committee of the Whole

REVISED STAFF REPORT

Agenda Item:		**Name:**	Nick Bowman
Proposed No.:	2021-0091	**Date:**	

COMMITTEE ACTION

***Proposed Substitute Ordinance 2021-0091.2 Prohibiting the acquisition and use of facial recognition technology by County administrative offices and executive departments passed out of committee on May 19, 2021, with a "Do Pass" recommendation. The Ordinance was amended in committee with Amendment S1 to* make technical corrections to the body of the ordinance as recommended by the Code Revisor.**

SUBJECT

Prohibiting the acquisition and use of facial recognition technology by County administrative offices and executive departments.

SUMMARY

Proposed Ordinance 2021-0091 would prohibit county administrative offices and executive departments from acquiring and using facial recognition technology or facial recognition information. County administrative offices and executive departments would also be prohibited from issuing any permit or entering into any agreement which authorizes any third party to use facial recognition technology or obtain facial recognition information on behalf of the county.

Facial recognition technology is defined as any computer software or application which assists in identifying an individual based on the physical characteristics of the individual's face. Facial recognition information is defined as any data or information obtained or derived from facial recognition technology

Violations of the Proposed Ordinance would constitute an injury to which a person subject to the violation may seek judicial relief.

BACKGROUND

Facial Recognition Technology. Facial recognition technology (FRT) is a category of biometric software[1] generally defined as a method of identifying or confirming an individual's identity using their face. Facial recognition can be used to identify people in photos, videos, or in real-time. While specific methods vary depending on the system provider, FRT generally includes the following processes:

- Capture: the process of finding an individual's face and removing the face from a larger image.
- Analysis: the process of mapping an individual's facial features/characteristics, such as the distance between a person's eyes, the depth of their eye sockets, the distance from forehead to chin, the shape of the cheekbones, and the contour of the lips, ears, and chin.
- Conversion: The process of taking the analyzed facial features and creating a standardized facial "template" or mathematical representation which can be compared to other facial templates housed in a reference database (often referred to as a gallery).
- Identification or Verification: The process of comparing a facial template against a database or gallery of other facial templates.
    - For an identification task, the facial recognition system is provided a probe image and attempts to match it with a biometric reference in a gallery.
    - For a verification task, an individual with a pre-existing relationship with an institution (and therefore already enrolled in the reference database or gallery) presents their biometric characteristics to the system (either a face or an image), claiming to be in the reference database or gallery (i.e. claiming to be a legitimate identity). The system then attempts to match the face or image with the claimed template in the reference database and either verifies or rejects the face or image.[2]

Automated facial recognition was developed in the 1960s, but did not really become widespread until the 2010s when computers became capable of training the neural networks required to make facial recognition a standard feature.[3] Today, facial recognition is used across the globe for a variety of purposes; from the relatively mundane, such as unlocking a smart phone and tagging a friend in a social media post, to the highly sophisticated, such as targeted advertising, law enforcement and surveillance.

A non-exhaustive list of FRT uses include:

- Accessing personal electronic devices and/or secure locations.
- Social media (i.e. tagging individuals in pictures/videos, "filter" applications, etc.).
- Law Enforcement:

---

[1] Other types of biometric software include voice recognition, fingerprint recognition, and eye retina or iris recognition.

[2] Introna, Lucas D. & Nissenbaum, Helen. (2010). "Facial Recognition Technology A Survey of Policy and Implementation Issues" New York University Center for Catastrophe Preparedness and Response. https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf

[3] Klosowski, Thorin. (July 15, 2020) "Facial Recognition Is Everywhere. Here's What We Can Do About It." https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/

    - Collecting arrestee mugshots and comparing them against local, state, and federal databases.
    - Querying mugshot databases to identify individuals in images.
    - Verifying the identity of wanted criminals or those suspected of a crime.
    - Locating missing persons and/or victims of human trafficking.
    - Identity theft and fraud detection.
- Streamline travel with "biometric passports" at border crossings and airports.
- Event registration.
- Individualized and targeted advertising/marketing.
- Retail theft prevention.
- Employee time and performance tracking.
- Banking.
- Healthcare.

Concerns.

The rapid advancement and sophistication of FRT in the last several years has raised concerns over its use. These concerns primarily focus on the accuracy of the technology, demographic biases, and encroachment on civil liberties.

Accuracy and Bias. FRT has proven effective with relatively small populations in controlled environments, for the verification of identity claims in which an image of an individual's face is matched to a pre-existing image "on-file" associated with the claimed identity (the verification task).[4] According to independent tests by the United States National Institute of Standards and Technology (NIST), between 2014 and 2018, the failure rate for finding a match in a database of twelve million portrait photos fell from 4% to 0.2%.[5] However, accuracy decreases when there is no standardized photo for comparison or when the comparison comes from a photo from an uncontrolled environment such as a face in a crowd image or a still from a live video feed. FRT works best when the picture is head-on and has no movement. Additionally, because faces change over time, unlike fingerprints or DNA, the technology can trigger incorrect results by changes in hairstyle, facial hair, body weight, and the effects of aging.[6]

Overall, the accuracy and reliability of FRT depends on several factors including:

- Environment: The conditions of the images to be compared (background, lighting, camera distance, and size and orientation of the head).
- Image Age: The time that has elapsed between the images to be compared.
- Consistent Camera Use: Similar optical characteristics of the camera used for the enrollment process and for obtaining the on-site image (light intensity, focal length, color balance, etc.).

---

[4] Introna, Lucas D. & Nissenbaum, Helen. (2010).

[5] Grother, Patrick. Ngan, Mei & Hanaoka, Kayee. (2018). "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification" National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8238

[6] Hamann, Kristine & Smith, Rachel. "Facial Recognition Technology: Where will it take us?" *Criminal Justice* Spring 2019. Pg. 9-13. https://pceinc.org/wp-content/uploads/2019/11/20190528-Facial-Recognition-Article-3.pdf

- Gallery Size: As the size of the gallery increases, the number of possible images that enter the gallery as near-identical mathematical representations (biometric doubles) also increases.[7]

Biases. Research has indicated that FRT may not be as accurate in reading the faces of certain demographic groups. FRT biases can occur when the neural networks of the system are trained on a data set of images which are not demographically balanced. When the system learns from a demographically uneven pool of images, the error rate for the demographic groups less represented in the data set increases.[8]

Research has shown that the demographic biases may be a product of the geographic region the FRT is developed. According to a 2011 NIST study of FRT algorithms developed in Western countries (France, Germany and the United States) and algorithms developed in East Asian countries (China, South Korea and Japan), Western algorithms recognized Caucasian faces more accurately than East Asian faces; and the East Asia algorithms recognized East Asian faces more accurately than Caucasian faces.[9]

More recent studies have shown that demographic biases persist, despite the general improvement in FRT in the last several years. A 2018 study testing three commercial face-analysis services found that the datasets were overwhelmingly composed of lighter-skinned subjects. As a result, the study found that darker-skinned females were the most misclassified group, with error rates of up to 34.7%, compared to the maximum error rate of 0.8% for lighter-skinned males.[10]

Civil Liberties. The use of FRT by governments and private enterprises, wherein individuals may have their faces scanned and added to a system's data set unknowingly and without consent, has raised concerns over the infringement on individual's right to privacy and other civil liberties. Civil rights and privacy organizations have argued that individuals have an expectation of anonymity in public settings and that few are privy to their identity and personal information. FRT erodes this expectation by allowing the user to identify an individual by their face and associate that individual's face with internet behavior, travel patterns, or other personal information.[11] Opponents have argued further that FRT may also allow unknown individuals or entities to track people's locations, movements, and companions and that information collected or associated with FRT could be used, shared, or sold in ways that people do not understand, anticipate, or consent to.[12]

---

[7] Introna, Lucas D. & Nissenbaum, Helen. (2010).

[8]Garvie, Clare & Frankle, Jonathan. "Facial-Recognition Software Might Have a Racial Bias Problem." The Atlantic. (April 7, 2016). https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/

[9] Phillips, P. , O'Toole, A. , Narvekar, A. , Jiang, F. and Ayadd, J. (2010), "An Other-Race Effect for Face Recognition Algorithms" National Institute of Standards and Technology, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904972

[10] Buolamwini, Joy & Gebru, Timnit. (2018) "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification"

[11] Geiger, Harley. "Facial Recognition and Privacy" Center for Democracy and Technology. https://cdt.org/insights/facial-recognition-and-privacy/

[12] Cackley, Alicia Puente (July 2015). "FACIAL RECOGNITION TECHNOLOGY Commercial Uses, Privacy Issues, and Applicable Federal Law"

Recent instances of FRT's use by law enforcement agencies have been cited by organizations such as the ACLU and the Electronic Freedom Foundation as examples of the threat posed by FRT to civil liberties. In 2016, the ACLU of Northern California reported that during protests surrounding the death of Freddie Gray, the Baltimore Police Department ran social media photos through face recognition technology to identify protesters and monitor them.[13] Also, in January 2020, a man named Robert Julian-Borchak Williams was arrested by the Detroit Police Department after being wrongly identified by the department's facial recognition system.[14]

Proponents of the technology point to instances where FRT has aided law enforcement in investigations and the apprehension of criminals. Once such instance is the August 2019 arrest of Larry Griffin II, who was arrested after being identified by a detective in the New York Police Department's Facial Identification Section on charges of placing fake bombs in a lower Manhattan subway station.[15] Other instances include FRT's assistance in recovering victims of human and sexual trafficking[16], and preventing foreign nationals from entering the United States using falsified or stolen U.S. passports.[17] More recently, federal court documents show the Federal Bureau of Investigation used FRT to assist in the identification of those individuals who participated in the January 6, 2021 riots at the U.S. Capitol in Washington D.C.[18]

Bans on Facial Recognition Technology. Citing many of the concerns listed above, several U.S. cities have banned municipal agencies from using FRT. As of November 2020, thirteen cities have enacted some form of FRT ban, including San Francisco, California, Boston, Massachusetts, Portland, Oregon, Portland, Maine, Jackson, Mississippi, and others.[19]

ANALYSIS

Proposed Ordinance 2021-0091 would ban the acquisition and use of facial recognition technology and facial recognition information by county administrative offices and

---

[13] Cagle, Matt. "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color." ACLU of Northern California. https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target

[14] Hill, Kashmir. "Wrongfully Accused by an Algorithm." The New York Times. (June 24, 2020). https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html?referringSource=articleShare

[15] McCarthy, Craig. "How NYPD's facial recognition software ID'ed subway rice cooker kook." The New York Post. (August 25, 2019). https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/

[16] Simonite, Tom. "How Facial Recognition Is Fighting Child Sex Trafficking." Wired. (June 19, 2019). http://wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/

[17] Sapp, Stephen. "Dulles CBP's New Biometric Verification Technology Catches Third Impostor in 40 Days." (October 20, 2018). https://www.cbp.gov/newsroom/national-media-release/dulles-cbp-s-new-biometric-verification-technology-catches-third

[18] Harwell, Drew & Timberg, Craig. "How America's surveillance networks helped the FBI catch the Capitol mob." The Washington Post. (April 2, 2021). https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/

[19] Flynn, Shannon. "13 Cities Where Police Are Banned From Using Facial Recognition Tech." Innovation and Tech Today. (November 18, 2020). https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/#:~:text=1.,facial%20recognition%20back%20in%202019.

executive departments.[20] The Proposed Ordinance would also prohibit county administrative offices and executive departments from issuing any permit or entering into any agreement which authorizes a third party to use facial recognition technology or obtain or access facial recognition information on behalf of the county. However, evidence relating to the investigation of a specific crime that may have come from facial recognition technology may be used by a county administrative office or executive department so long as the evidence was not generated by or at the request of the county office or department.

The Proposed Ordinance defines facial recognition technology as any computer software or application which assists in identifying, or verifying the identify of, an individual based on the physical characteristics of the individual's face. Facial recognition technology does not include the analysis of facial features to grant access to an electronic device or the use of redacting software to protect the privacy of an individual depicted in a recording intended for release or disclosure. Facial recognition information is also defined as any data or information obtained or derived from facial recognition technology.

The Proposed Ordinance would establish a process for county personnel who inadvertently or unintentionally use or access facial recognition information. County personnel is defined to include any person or entity acting on behalf of the county whether an officer, employee, agent, contractor, subcontractor vendor or volunteer. This process would require county personnel to notify their direct supervisor that they received, used, or gained access to facial recognition information and that they immediately delete the information subject to applicable laws.

Any facial recognition information collected or derived in violation of the established ban would be considered unlawfully obtained. Violations of the established ban on the use of facial recognition technology and/or information would constitute an injury to which a person subject to the violation may seek relief in any court of competent jurisdiction. Furthermore, a prevailing plaintiff in any such court proceeding would be entitled to awarded costs and reasonable attorney fees.

Comparison with Washington State Law

In 2020, the Washington State Legislature adopted Engrossed Substitute Senate Bill 6280 concerning the use of facial recognition services. Table 1 below provides a comparison of the state law to the Proposed Ordinance.

Table 1. State Law Versus Proposed Ordinance 2021-0091

Provisions	State Law	PO 2021-0091

[20] King County Charter Section 350 defines county administrative offices as "those agencies of the executive branch which provide administrative services for the various agencies of county government," and executive departments as "the department of assessments, the department of judicial administration, the department of elections, the department of public defense and those agencies of the executive branch which are primarily engaged in the execution and enforcement of ordinances and statutes concerning the public peace, health and safety and which furnish or provide governmental services directly to or for the residents of the county." The Department of Public Safety, otherwise known as the King County Sheriff's Office, is also included the list of executive departments under Charter Section 350.20.40.

Definitions	• Facial Recognition Service: means technology that analyses facial features and is used by a state or local government agency for the identification, verification, or persistent tracking of individuals in still or video images. • Facial Recognition Service does not include: The analysis of facial features to grant or deny access to an electronic device; or the use of an automated or semiautomated process for the purpose of redacting a recording for release or disclosure.	• Facial Recognition Technology: means any computer software or application which assists in identifying, or verifying the identify of, an individual based on the physical characteristics of the individual's face. • Facial Recognition Technology does not mean: the analysis of facial features to grant access to an electronic device or the use of redacting software to protect the privacy of an individual depicted in a recording intended for release or disclosure.
Government Review	• Any state or local government using or intending to use FRT must notify a legislative authority and provide that authority with an Accountability Report, which must include a description of the proposed use and capabilities of the service, information on the service's rate of false matches, data security measures, procedures regarding testing and channels for receiving feedback, and data integrity and retention policies i.e. how long data will be held. • Prior to finalizing the Accountability Report, a government agency must: allow for public review and comment, hold at least three community consultation meetings, and consider issued raised by the public. • The final Accountability report must be subject to a public review period and be updated every two years.	NA

	• The final adopted Accountability Report must be clearly communicated to the public at least 90 days before the FRT is put into operational use.	
Meaningful Human Review	Any government agency wishing to use FRT in a manner which assists in making decisions that produce legal effects i.e. provision or denial of financial and lending services, housing, insurance, education, criminal justice etc., must ensure that those decisions are subject to meaningful human review.	NA
Independent Testing	A government agency using FRT require a service provider to make available an application programming interface (API) to enable independent testing for accuracy and unfair performance differences across distinct subpopulations. If results of the independent testing identify material unfair performance differences across subpopulations the provider must develop and implement a plan to mitigate the identified performance differences within 90 days of receipt of such results.	NA
Operational Testing	Prior to deploying FRT, an agency using FRT to make decisions that produce legal effects or similarly significant effects on individuals must test a service in operational conditions.	NA
Training	A government agency using FRT must conduct periodic training of all individuals who operate a service or who process personal data obtained from the use of a service	NA
Prohibitions	• A government agency may not use FRT to engage in ongoing surveillance, conduct real-time or near-real time identification, or start persistent tracking unless: a warrant is obtained; exigent circumstances exist; or a court order is obtained for the sole purpose of locating or identifying a	Proposed Ordinance 2021-0091 would prohibit the use of FRT by any County Administrative Office or Executive Department.

	missing person, or identifying a deceased person. • An agency may not: apply a service to any individual based on certain characteristics protected by law; or use a service to create a record describing any individual's exercise of rights guaranteed by the 1st Amendment rights. • Law enforcement agencies may not: use the results of FRT as the sole basis to establish probable cause in a criminal investigation; use a service to identify an individual based on a sketch or manually produced image; or substantively manipulate an image for use in a service in a manner not consistent with the service provider's intended use and training.	
Inadvertent Use	NA	County personnel who inadvertently use or access FRT must notify their direct supervisor that they received, used, or gained access to facial recognition information and that they immediately delete the information subject to applicable laws.
Exemptions	• The provisions of the state law do not apply to any government agency who is mandated to use FRT pursuant to a federal regulation or order; or uses FRT in association with a federal agency to verify the identity of individuals presenting themselves for travel in an airport or seaport. • The law does not apply to the use of a facial recognition matching system by DOL authorized under current law.	• Evidence relating to the investigation of a specific crime that may have come from facial recognition technology may be used by a county administrative office or executive department so long as the evidence was not generated by or at the request of the county office or department. • The PO does not prohibit the use of social media or communications software, or automated redaction software, provided such

		software does not have the facial recognition capabilities. • The PO does not prohibit any County entity from complying with the National Child Search Assistance Act.

Questions from May 5, 2021 Committee of the Whole Meeting

Responses to the questions raised during the May 5, 2021 Committee of the Whole meeting will be distributed prior to the May 19, 2021 committee meeting.

AMENDMENT

Striking Amendment S1 makes technical corrections to the body of the ordinance.