

**Special Commission to Evaluate Government Use of Facial
Recognition Technology in the Commonwealth**

Final Report

March 14, 2022

Note from Chairs

In addition to the valuable contributions from the Commissioners, the Chairs acknowledge and thank the work of their legislative staff, without whom the Special Commission on Government Use of Facial Recognition Technology in the Commonwealth could not have completed its work. The staff of the Committee on the Judiciary drafted and compiled the minutes of all Commission meetings; created and maintained a robust public website containing meeting agendas and minutes, materials considered by the Special Commission and public testimony offered to the Special Commission; coordinated the logistics of all Commission Meetings; scheduled and worked with individuals making presentations to the Commission; greatly contributed to the drafting of the Final Report; and coordinated and tallied the final votes of the Commission.

The Special Commission could not have met its statutory charge without the dedication and hard work of Judiciary Committee General Counsel Dianna Williams, Staff Director Patrick Prendergast, Research and Communications Director Jacqueline Manning, and Senate Chief of Staff Michael Carr and General Counsel David Emer. The Chairs are grateful for the talents of these dedicated public servants.



Michael S. Day, Co-Chair
Special Commission on Government Use
of Facial Recognition Technology
in the Commonwealth



Jamie Eldridge, Co-Chair
Special Commission on Government Use
of Facial Recognition Technology
in the Commonwealth

Commission Membership¹²

- **Representative Michael S. Day, *Co-Chair***; House Chair of Joint Committee on the Judiciary
- **Senator James B. Eldridge, *Co-Chair***; Senate Chair of Joint Committee on the Judiciary
- **Representative David M. Rogers**; Appointed by Speaker of House of Representatives
- **Professor John D. Woodward, Jr.**; Appointed by Speaker of House of Representatives
- **Professor Woodrow Hartzog**; Appointed by Speaker of House of Representatives
- **Senator Adam Gomez**; Appointed by Senate President
- **Senator Cynthia Stone Creem**; Appointed by Senate President
- **Professor Maurice R. Dyson**; Appointed by Senate President
- **Chief William G. Brooks, III**; Designee of House Minority Leader
- **Ret. Associate Justice Robert J. Cordy**; Designee of Senate Minority Leader
- **Alicia Rebello-Pradas, Esq.**; Chief, Policy & Government (Relations) Division, Office of the Attorney General; Designee of the Attorney General
- **Chief Jeff Farnsworth**, Senior Policy Advisor, Executive Office of Public Safety and Security; Designee of the Secretary of Public Safety and Security
- **Registrar Colleen Ogilvie**; Registrar of Motor Vehicles
- **Kade Crockford**; Designee of the Executive Director of the ACLU of Massachusetts
- **Matthew Spurlock, Esq.**; Designee of the Chief Counsel of the Committee for Public Counsel Services
- **Mutale NKonde**; Designee of the President of NAACP New England Area Conference
- **Charu A. Verma, Esq.**; Designee of the Chief Legal Counsel of the Massachusetts Bar Association
- **Major Mark D. Cyr**; Designee of the Colonel of Massachusetts State Police³
- **District Attorney Michael D. O’Keefe**; Cape & Islands; Designee of the President of the Massachusetts District Attorneys Association
- **Chief Edward G. Conley**; Designee of the President of the Massachusetts Chiefs of Police Association
- **Professor Erik G. Learned-Miller**; Designee of Governor Charles D. Baker

¹ The Commissioner Vote Record on the Final Report can be found in the Appendices as Appendix A.

² Section 105(a) of Chapter 253 of the Acts of 2020 appointed Chief Justice of the Supreme Judicial Court or her designee as an additional member to this commission. However, by letter dated May 4, 2021, Chief Justice Kimberly S. Budd advised the chairs that she was unable to serve or make a designation to the commission. A copy of that letter is included in Appendix B.

³ The Colonel of the Massachusetts State Police’s initial designee was Major Scott Range. Major Range retired in September 2021 and Major Cyr was thereafter designated by the Colonel by letter dated October 7, 2021.

TABLE OF CONTENTS

I.	Statutory Charge	5
II.	Introduction	7
III.	Facial Recognition Explained	9
IV.	The Use of Facial Recognition in Massachusetts	11
V.	The Regulation of Facial Recognition in Massachusetts	13
	a. Facial Recognition in Massachusetts before Police Reform	13
	b. Chapter 253 of the Acts of 2020 (“Police Reform”)	13
	c. Use of Facial Recognition after Police Reform	16
	d. Facial Recognition Regulation by Massachusetts Municipalities	17
	e. Legislation in Other Jurisdictions	17
VI.	Advantages and Disadvantages of Facial Recognition	21
	a. Utility of Facial Recognition	22
	b. Concerns with Facial Recognition	23
	i. Accuracy Concerns	23
	ii. Constitutional/Due Process Concerns	26
	iii. Privacy Concerns	28
VII.	Deliberations	28
VIII.	Recommendations	29
IX.	Appendices	34
	a. Appendix A: Commissioner Vote Record on Final Report	35
	b. Appendix B: Letter from Supreme Judicial Court Chief Justice Budd	37
	c. Appendix C: Meeting Minutes	40
	d. Appendix D: Initial Survey Template	62
	e. Appendix E: Summary of Initial Survey Responses	65
	f. Appendix F: Follow-Up Survey Template	71
	g. Appendix G: Follow-Up Survey Responses	75
	h. Appendix H: Department of State Police Policy and Procedure	169
	“Use of Facial Recognition Technology”	

I. Statutory Charge

Section 105 of Chapter 253 of the Acts of 2020:

(a) Notwithstanding any special or general law to the contrary, there shall be a special legislative commission established pursuant to section 2A of chapter 4 of the General Laws to conduct a study on government use of facial recognition technology in the commonwealth.

The commission shall consist of 22 members: 2 of whom shall be the chairs of the joint committee on the judiciary or their designees, who shall serve as co-chairs; 3 of whom shall be appointed by the president of the senate; 3 of whom shall be appointed by the speaker of the house of representatives; 1 of whom shall be the minority leader of the house of representatives or a designee; 1 of whom shall be the minority leader of the senate or a designee; 1 of whom shall be the chief justice of the supreme judicial court or a designee; 1 of whom shall be the attorney general or a designee; 1 of whom shall be the secretary of public safety and security or a designee; 1 of whom shall be the registrar of motor vehicles or a designee; 1 of whom shall be the executive director of the American Civil Liberties Union of Massachusetts, Inc. or a designee; 1 of whom shall be the chief counsel for the committee for public counsel services or a designee; 1 of whom shall be the president of the National Association for the Advancement of Colored People New England Area Conference or a designee; 1 of whom shall be the chief legal counsel for the Massachusetts Bar Association or a designee; 1 of whom shall be the colonel of state police or a designee; 1 of whom shall be the president of the Massachusetts District Attorneys Association or a designee; 1 of whom shall be the president of the Massachusetts Chiefs of Police Association Incorporated or a designee; 1 of whom shall be an academic expert in: (i) data science, artificial intelligence and machine learning; (ii) social implications of artificial intelligence and technology; or (iii) information policy, technology and the law, to be appointed by the governor.

The commission shall evaluate government use of facial recognition technology in the commonwealth and make recommendations to the legislature regarding appropriate regulations, limits, standards and safeguards. The commission shall:

- (i) survey current government uses of facial recognition technology in the commonwealth;
- (ii) consult with academic experts in the fields of machine learning, algorithmic bias, criminal law, and human rights;
- (iii) examine research regarding the ability of facial recognition technology to accurately identify people of different races, genders and ages;
- (iv) examine and evaluate the facial recognition system operated by the registry of motor vehicles, make recommendations for regular independent bias testing and propose standards to ensure accuracy and equity of the system based on age, race, gender and religion;

(v) examine access to the facial recognition system operated by the registry of motor vehicles and the management of information derived from it, including, but not limited to, data retention, data sharing and audit trails;

(vi) evaluate current access by federal agencies to databases maintained by the commonwealth that catalogue images of faces and examine which agencies have such access, and the authorization for, and terms of, such access;

(vii) evaluate a requirement for law enforcement agencies to obtain a probable cause warrant prior to performing facial recognition searches, including the merits of requiring enhanced standards to perform a search similar to those set forth in section 99 of chapter 272 of the General Laws;

(viii) examine whether, and under what circumstances, it is appropriate for law enforcement agencies to perform facial recognition searches without a warrant, and make recommendations for safeguards regarding due process, accountability, oversight, documentation and transparency for any such searches;

(ix) provide recommendations for any necessary due process protections for criminal defendants when facial recognition technology is used in a criminal investigation;

(x) provide recommendations to ensure privacy for the public, including, but not limited to, the use of facial recognition to conduct surveillance of people in public spaces; and

(xi) provide recommendations for adequate training and oversight on the use of facial recognition technology.

For the purposes of this section, “facial recognition” shall mean an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual’s face, head or body, that uses characteristics of an individual’s face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that “facial recognition” shall not include the use of search terms to sort images in a database.

(b) The executive office of public safety and security shall, at the request of the commission, provide to the commission timely access to all information to be published in the annual report pursuant to subsection (d) of section 220 of chapter 6 of the General Laws.

(c) The commission shall convene beginning not later than February 15, 2021, and shall submit its findings and recommendations, including any proposed legislation, relative to the use of facial recognition technology by filing the same with the clerks of the house of representatives and senate and the governor not later than December 31, 2021.

II. Introduction

Facial recognition is a biometric technology⁴ that uses distinguishable facial features to identify a person. The scope and potential of this technology is profound and it is already used in a wide variety of applications in the public and private sector. The Major Cities Chiefs of Police Association (“MCCA”) has noted, “[f]acial recognition technology is being used daily to aid law enforcement in capturing the most violent criminals in our country and bringing closure for victims. It has been proven to be highly successful in solving various types of crimes afflicting our communities when used with the highest degree of responsibility, transparency, and accountable management.”⁵

However, with such powerful technology comes the risk of misuse and abuse. Each facial recognition system is different, all have inherent accuracy concerns, and different systems are better suited for certain applications under specific conditions. Facial recognition also potentially poses a significant threat to fundamental civil rights and constitutional freedoms if misused by government actors. The unregulated and unmonitored use of facial recognition technology by the government, and especially by law enforcement, is concerning when viewed through a civil liberties prism.

Advocates and critics of facial recognition have differing views on law enforcement use of this technology. The ACLU of Massachusetts noted in testimony submitted to the Commission, “[a]dvanced technologies can be effectively used to solve crimes, no doubt. But surveillance technologies like facial recognition also give the government vast new powers to invade our privacy, monitor our speech and association, and digitize and automate racial profiling. Therefore, the legislature must impose safeguards to prevent government from abusing its power, or misusing technology in ways that harm individuals and communities.” However, Commissioner Brooks, Chief of the Norwood Police Department, countered:

There are concerns among some members of the public about the use of FR by the police, but I believe that most of those concerns stem from a lack of understanding of how the technology is actually applied. I believe it is useful to think about FR as analogous to an anonymous tip line, a tool that police have used for decades. When someone calls the police tip line and says that detectives should take a look at Bob Jones for a recent robbery, the police take that information as a potential lead, but it is clearly not evidence. The tip cannot be introduced in court, for obvious reasons. Instead, the police take the information

⁴ ‘Biometric surveillance system,’ is defined as “any computer software that performs facial recognition or other remote biometric recognition.” Section 26 of Chapter 253 of the Acts of 2020. ‘Other remote biometric recognition’ is defined as “an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on an individual’s gait, voice or other biometric characteristic or that uses such characteristics to infer emotion, associations, activities or the location of an individual; provided, however, that ‘other remote biometric recognition’ shall not include the identification or verification of an individual using deoxyribonucleic acid, fingerprints, palm prints or other information derived from physical contact.” Id.

⁵ See 2021 Facial Recognition Working Group, Major Cities Chiefs of Police, “Facial Recognition Technology in Modern Policing: Recommendations and Considerations” (2021).

and check to see whether Jones might be the offender. Perhaps his fingerprints are in the stolen car that was recovered, or an eyewitness selects him from a photo array. But the tip itself is never introduced; the detective cannot even mention it in his or her testimony. By the same token, if the tip never pans out- there is nothing to connect Jones to the holdup- then nothing ever comes out of the tip. The fact that the police have a tip line will not cause a wrongful conviction.

On December 31, 2020, the Commonwealth of Massachusetts enacted Chapter 253 of the Acts of 2020, entitled *An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth* (the “Police Reform Law”). Section 105(a) of this Act created a special legislative commission to study government use of facial recognition technology in the Commonwealth. More specifically, the law directed the commission to review how facial recognition is used by the government in Massachusetts, investigate accuracy, privacy, and due process concerns surrounding the use of this technology, and make recommendations to address these concerns and improve accuracy, training, transparency, and oversight.

“Facial recognition” is defined in Section 105(a) as “an automated to semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual’s face, head or body, that uses characteristics of an individual’s face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that ‘facial recognition’ shall not include the use of search terms to sort images in a database.”

The Commission convened in early 2021 and met on eight occasions between April 16 and December 17.⁶ As part of its work, the Commission accepted written and oral testimony, reports, articles, and other supporting materials from a host of individuals and groups, including but not limited to: ACLU of Massachusetts, Boston Teachers Union, Boston City Council, Council on American-Islamic Relations, Clearview AI, Digital Fourth, Electronic Frontier Foundation, GLAAD, League of Women Voters of Massachusetts, LivableStreets Alliance, NAACP New England Area Conference, National Child Protection Task Force, Pirate Party, Progressive Massachusetts, and Project on Government Oversight. The Commission welcomed presentations from several Commissioners, including Professor Erik Learned-Miller of UMass Amherst, Registrar Colleen Ogilvie of the Registry of Motor Vehicles, Major Scott Range of the Massachusetts State Police, and Kade Crockford of the ACLU of Massachusetts. The Commission reviewed limitations imposed on the use of facial recognition in municipalities in the Commonwealth and other jurisdictions in the United States. The Commission also distributed a set of surveys to law enforcement and prosecuting agencies in the Commonwealth to gain better insight into their prior and current use of facial recognition. The following report represents a culmination of the Commission’s deliberations and findings that were informed from those discussions, presentations, testimony, documentation, and research.

⁶ To view the recordings of all Commission meetings, visit <https://malegislature.gov/Commissions/Detail/549/Hearings>. To view Commission agendas, minutes, written testimony, and other submissions, visit <https://frcommissionma.com/>. Meeting minutes are also included in Appendix C.

III. Facial Recognition Explained

On May 21, 2021, Commissioner Erik Learned-Miller gave an introductory presentation to the Commission on facial recognition.⁷ Commissioner Learned-Miller also provided a primer and white paper he and his colleagues prepared to supplement his presentation.⁸

The terms ‘face recognition’ and ‘facial recognition’ are often used interchangeably to refer to “the process of using digital representations of faces to try to identify or verify the identity of a unique individual.”⁹ There are two primary types of facial recognition: face verification and face identification.¹⁰

Face verification, which is also referred to as 1-to-1 matching or 1-to-1 comparison, seeks to determine whether an image shows a specific person:

There are two common ways to perform face verification. In the first, one asks a question such as “Does this image show Janelle Smith?”, in which the person of interest is named. To answer this question, a system needs some prior source of information about the appearance of Janelle Smith, such as previously obtained pictures or a description. A common use for this type of face verification is access control, such as software that allows the owner of a device or a service to access it. Access control can be used to unlock a phone, access a bank account, or pay for an item with a digital currency. If you use face verification to access your cell

⁷ Commissioner Learned-Miller, a professor of computer science at UMass Amherst, has researched facial recognition since 2006, during which time he developed one of the most widely used benchmarks for measuring face recognition accuracy and developed the top face recognizer and face detector in the world. *See* Erik Learned-Miller, “Face Recognition Technology: Background for the Massachusetts Facial Recognition Commission” [Commission Presentation], Special Commission on Facial Recognition Meeting (May 21, 2021), <https://malegislature.gov/Events/Hearings/Detail/3729>.

⁸ *See* Joy Buolamwini, Vicente Ordóñez, Jamie Morgenstern, and Erik Learned-Miller, Facial Recognition Technologies: A Primer (May 29, 2020), <https://frcommissionma.files.wordpress.com/2021/06/frtprimer.pdf>; and Erik Learned-Miller, Vicente Ordóñez, Jamie Morgenstern, and Joy Buolamwini, Facial Recognition Technologies in the Wild: A Call for a Federal Office (May 29, 2020), <https://frcommissionma.files.wordpress.com/2021/06/frtinthewild.pdf>.

⁹ The image of a particular individual used in a facial recognition search is often referred to as the ‘query image,’ ‘probe image,’ ‘query,’ or ‘probe.’ Facial Recognition Technologies: A Primer, *supra* at 5.

¹⁰ MCCA’s report also includes a third type of facial recognition called field verification. “Field verification is the use of FRT in the field for the purpose of identifying an individual during a live interaction. This mode of FRT is primarily used to attempt to ‘fill the gaps’ in available information such as when a subject lacks formal issued identification or is uncooperative and refuses to give proper identification. This type of FRT can aid in confirming who a subject is claiming to be.” 2021 Facial Recognition Working Group, Major Cities Chiefs of Police, “Facial Recognition Technology in Modern Policing: Recommendations and Considerations” (2021).

phone, the face verification system takes a new picture of your face (the query image) and compares it to information it obtained previously to try to assess whether you are the same person...In the second common version of face verification, one is given two pictures and asks, “Is the first person the same as the second person?” In this case, it is not necessary to know the identity of either person to answer the question.¹¹

In law enforcement, face verification can be useful in correctional facilities to grant access to secured areas, confirm inmate identity in a booking or release environment, or confirm identity at border crossings.¹²

Face identification, also known as image matching, one-to-many comparison, one-to-many matching, one-to-many identification, or one-to-N identification, attempts to identify the person in an image:

Face identification attempts to answer the question, “Whose face is this?” Face identification software can only match the image of a face to a person for whom it already has some appearance information. The set of people for whom an application has stored appearance information is called the gallery. Simply put, this is the set of people that a face identification system could possibly identify. A typical example of a gallery would be the set of people who work in a secured location, such as a private office building. The correct answer to a face identification query is either the identity of a person in the gallery (e.g., “Employee #347”) or “none of the above” if the image shows a person who is not in the gallery.¹³

Facial identification is the most common type of facial recognition used by law enforcement and is the application most criticized.

Once an image is taken and a face is detected in the image, characteristics of the face may be stored in a numerical format called a faceprint.¹⁴ When a machine compares two faceprints, a similarity score, also referred to as a confidence level, may be computed to represent the similarity of the faceprints (e.g., 0-100%). This score is not perfect, though “generally speaking, the higher the similarity score the more likely the faceprints being compared belong to the same individual.”¹⁵

¹¹ Id. at 5-6.

¹² *See* Facial Recognition Technology in Modern Policing: Recommendations and Considerations, *supra*.

¹³ Id. at 6.

¹⁴ Id. at 10.

¹⁵ Id. at 12.

A developer or user of a facial recognition system can set a threshold similarity score to only produce close matches. For example, “if a system returns a similarity score between 0 and 100 and a threshold of 80 is set, only faceprints with similarity scores at or above 80 are considered a match.” For face verification (1-to-1 comparison), the results of a search will be either a match or no match based on the threshold set. For face identification (1-to-many comparison), a query may return zero matches, one match or multiple matches.¹⁶ If a search generates multiple matches, a human reviewer is often utilized to examine the results more closely and determine whether any are actual or likely matches.

In addition to the above technical definition of facial recognition, which includes face verification and face identification, the term is often used more broadly as a catchall phrase for related biometric technologies. This includes face attribute classification or estimation, which assesses the attributes of a person, like gender, race, ethnicity, or age, from their face. This also includes emotion, affect, and facial expression classification, which classifies facial expressions, like a smile, frown, or scowl, to infer the emotional state or affect of a person, like happy, sad, angry, or deceitful. Beyond set images, these technologies can be applied to live surveillance¹⁷ to track and catalogue an individual’s movements, habits, and associations.

IV. The Use of Facial Recognition in Massachusetts

In accordance with its charge, the Commission reviewed the use of facial recognition by the government at large in Massachusetts, including in schools¹⁸ and airport security,¹⁹ and discussed the potential for even greater use of the technology in the future. However, the

¹⁶ *Id.* at 13.

¹⁷ MCCA noted in its report: “FRT platforms have the capability of being used as a surveillance tool by identifying persons in real-time using video feeds layered with FRT technology. Known instances of this type of use of FRT can be found in foreign nations and among certain private sector businesses.” Facial Recognition Technology in Modern Policing: Recommendations and Considerations, *supra*.

¹⁸ The Boston Teacher’s Union, in testimony submitted to the Commission, confirmed the use of facial recognition technology in Boston schools and noted that “[o]ur schools are places where parents or students who don’t feel comfortable with the immigration system and the criminal justice system, do engage with teachers, administrators, counselors, etc. on behalf of their kids, or on behalf of their own education. Installing facial or other biometric recognition software in schools runs counter to that purpose, and could keep parents and students away from the very institutions that can do more than any other to help them.” Additionally, the Commission noted several news articles suggesting the use of facial recognition in other schools in Massachusetts. *See* Ryan Mac, Caroline Haskins, and Logan McDonald, “Clearview’s Facial Recognition App Has Been Used By The Justice Department, ICE, Macy’s, Walmart, And The NBA,” BuzzFeed News (February 27, 2020, at 11:37 PM ET), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

¹⁹ U.S. Government Accountability Officer, Facial Recognition Technology: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues, September 2020, <https://www.gao.gov/assets/gao-20-568.pdf>.

Commission's conversations and discussions focused primarily on law enforcement use of the technology.

To better understand the scope and frequency of the use of facial recognition by law enforcement, the Commission sent a set of surveys to law enforcement and prosecuting agencies in the Commonwealth. The Commission distributed an initial survey on or about August 25, 2021 ("Initial Survey") to 357 local law enforcement agencies, eleven district attorney's offices, the Massachusetts State Police ("MSP"), and the Registry of Motor Vehicles ("RMV").²⁰ As of December 31, 2021, the Commission received 167 responses,²¹ including from 156 local law enforcement agencies, nine district attorney's offices, the MSP, and the RMV.²²

Out of 166 offices and departments surveyed, 80.4% (131 responders) reported that they do not currently use facial recognition and have no plans to use it; twelve reported that they do not currently use facial recognition but have plans to use it; eleven reported that they used or tested facial recognition, but no longer use or test it; nine reported that they currently use facial recognition; and three responders failed to respond to this question.

Of those who reported using facial recognition, either previously or currently, most offices and departments reported relatively infrequent use: eleven reported conducting 0-5 searches; two reported conducting 6-10 searches; one reported conducting 11-20 searches; two reported conducting 20-50 searches; and two reported conducting 51 or more searches.²³

The Commission then sent a follow-up survey ("Follow-Up Survey") to the twenty departments that reported previously or currently using facial recognition.²⁴ As of December 31,

²⁰ The Initial Survey is included in Appendix D.

²¹ A summary of the responses to the Initial Survey is included in the Appendices as Appendix E.

²² The RMV provided a separate written response to the Initial Survey which stated, in part: "The RMV has used facial recognition technology since approximately 2006...[T]he RMV relies on facial recognition technology to protect the integrity of the identification and driver licensing credentials it issues. Use of facial recognition technology in the credential issuance process helps the RMV to identify and correct simple administrative errors, ensure that each customer's identity has not been misused by another person, and uncover any other forms of potentially fraudulent activity...The RMV's civilian analysts and hearings officers do not use the RMV's facial recognition technology to assist other state or Federal agencies with criminal investigations that are unrelated to RMV credential fraud. Instead, the RMV refers any such requests by these agencies to the MSP, since entering into a Memorandum of Understanding between the RMV and the MSP."

²³ The MSP, who reported currently using facial recognition, did not respond to the Initial Survey question asking how many searches they conducted. Ashby Police Department did not respond to this question either. However, while Ashby's Initial Survey response stated that it previously used but no longer uses facial recognition, its Follow-Up Survey response stated that it has not used facial recognition, suggesting that the Initial Survey response may have been erroneous.

²⁴ This included the nine offices/departments that stated in their Initial Survey that they currently use facial recognition and the eleven departments that stated they previously used facial recognition but no longer do so.

2021, the Commission received responses from fourteen departments.²⁵ Responding agencies reported using both governmental and third-party facial recognition systems, including Clearview AI, CrimeDex, CopLink, NESPIN, Spotlight, Rhode Island State Fusion Center, RMV, and most predominantly the Massachusetts State Fusion Center.

Notably, in addition to the roughly 200 local law enforcement agencies who did not respond to the Initial Survey, the above statistics do not include the many federal law enforcement agencies operating in Massachusetts. On June 29, 2021, the U.S. Government Accountability Office (“GAO”) publicly released a report reviewing federal law enforcement use of facial recognition technology.²⁶ GAO surveyed 42 federal agencies employing law enforcement officers about their use of facial recognition technology. Twenty agencies reported owning facial recognition systems or using systems owned by others, of whom fifteen reported using non-federal systems.

V. The Regulation of Facial Recognition in Massachusetts

a. Facial Recognition in Massachusetts before Police Reform

While there have been a number of legislative proposals on both the federal and state level to do so, no state or federal law regulated the government’s use of facial recognition technology prior to the enactment of the Police Reform Law on December 31, 2020. Furthermore, apart from the MSP,²⁷ of the fourteen law enforcement agencies that responded to the Follow-Up Survey, no agency reported having any standards or guidelines in place for the use of facial recognition. Instead, most reported deferring to the entity running the facial recognition search to make determinations regarding image quality and match accuracy. The Commission found this alarming and problematic.

b. Chapter 253 of the Acts of 2020 (“Police Reform”)

On December 31, 2020, Massachusetts enacted the Police Reform Law. This sweeping legislation sought to increase training, oversight, accountability, and transparency in order to restore trust and confidence in law enforcement. Among the measures included were the standardization of training standards and policies for all law enforcement in the Commonwealth, the update of use of force policies to explicitly prohibit chokeholds and impose a duty to intervene, the organization and centralization of training, certification, employment, and internal affairs records, and the creation of the Massachusetts Peace Officer Standards and Training

²⁵ The Follow-Up Survey is included in Appendix F. Responses to the Follow-Up Survey are included in Appendix G.

²⁶ U.S. Government Accountability Officer, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks, June 3, 2021. <https://www.gao.gov/products/gao-21-518>

²⁷ The MSP’s prior standard operating procedure is included in its response to the Follow-Up Survey in Appendix G and its current procedure is included in Appendix H.

Commission (“POSTC”), a statewide, majority-civilian oversight board empowered to certify and decertify law enforcement professionals based on training and conduct.

The Police Reform Law also imposed certain restrictions on the use of facial recognition²⁸ by law enforcement agencies²⁹ in the Commonwealth. Section 26 of the law provides that any law enforcement agency performing or requesting a facial recognition search using facial recognition technology shall only do so through a written request submitted to the RMV, MSP, or FBI.³⁰ A law enforcement agency may only perform a facial recognition search for the following purposes:³¹

- (i) to execute an order, issued by a court or justice authorized to issue warrants in criminal cases, based upon specific and articulable facts and reasonable inferences therefrom that provide reasonable grounds to believe that the information sought would be relevant and material to an ongoing criminal investigation or to mitigate a substantial risk of harm to any individual or group of people; or
- (ii) without an order to identify a deceased person or if the law enforcement agency reasonably believes that an emergency involving substantial risk of harm to any individual or group of people requires the performance of a facial recognition search without delay. Any emergency request shall be narrowly tailored to address the emergency and shall document the factual basis for believing that an emergency requires the performance of a facial recognition search without

²⁸ The definition of ‘facial recognition’ in Section 26 is the same as the definition contained in Section 105 of Chapter 253 of the Acts of 2020, *supra*.

²⁹ ‘Law enforcement agency’ is defined as “(i) a state, county, municipal or district law enforcement agency, including, but not limited to: a city, town or district police department, the office of environmental law enforcement, the University of Massachusetts police department, the department of the state police, the Massachusetts Port Authority police department, also known as the Port of Boston Authority police department, and the Massachusetts Bay Transportation Authority police department; (ii) a sheriff’s department in its performance of police duties and functions; or (iii) a public or private college, university or other educational institution or hospital police department.” See Section 26(a) of Chapter 253 of the Acts of 2020; Section 30 of Chapter 253 of the Acts of 2020.

³⁰ See Section 26(b) of Chapter 253 of the Acts of 2020.

³¹ This section does not apply to investigatory functions performed by the MSP related to the issuance of identification documents. Section 26(b) of Chapter 253 of the Acts of 2020. Additionally, a law enforcement agency may: (i) acquire and possess personal electronic devices, such as a cell phone or tablet, that utilizes facial recognition technology for the sole purpose of user authentication; (ii) acquire, possess and use automated video or image redaction software; provided, that such software does not have the capability of performing facial recognition or other remote biometric recognition; and (iii) receive evidence related to the investigation of a crime derived from a biometric surveillance system; provided, that the use of a biometric surveillance system was not knowingly solicited by or obtained with the assistance of a public agency or any public official in violation of subsection (b). Section 26(e) of Chapter 253 of the Acts of 2020.

delay.³²

Additionally, Section 26 imposes reporting requirements on law enforcement agencies and the Executive Office of Public Safety and Security (“EOPSS”). Section 26(c) requires law enforcement agencies to document each facial recognition search performed and provide this documentation quarterly to EOPSS. This documentation must include:

- (i) a copy of any written request made for a facial recognition search;
- (ii) the date and time of the request;
- (iii) the number of matches returned, if any;
- (iv) the database searched;
- (v) the name and position of the requesting individual and employing law enforcement agency;
- (vi) the reason for the request, including, but not limited to, any underlying suspected crime;
- (vii) the entity to which the request was submitted; and
- (viii) data detailing the individual characteristics included in the facial recognition request.³³

EOPSS must publish this information on its website annually, not later than September 1,³⁴ along with the following data for the previous calendar year:

- (i) the total number of facial recognition search requests made by other law enforcement agencies to the department of state police, disaggregated by law enforcement agency;
- (ii) the total number of facial recognition searches performed by the department of state police, disaggregated by law enforcement agency on whose behalf the search was performed;
- (iii) the total number of facial recognition searches requested and performed by the state police;
- (iv) the total number of facial recognition search requests made by the department of state police to the Federal Bureau of Investigation, disaggregated by law enforcement agency on whose behalf the requests were made; and

³² Id.

³³ Id.

³⁴ The Commission recognized that EOPSS published its first required annual report on or about September 1, 2021. However, this report provided very limited information, noting that, “[b]ecause G.L. c. 6, § 220 became effective on July 1, 2021, and because G.L. c. 6, § 220(c) requires law enforcement agencies to provide documentation quarterly, EOPSS has not yet received any quarterly reports from law enforcement agencies...” The Commission requested updated information by letter dated October 26, 2021, but, as of December 31, 2021, has not received a response.

- (v) the total number of facial recognition searches performed by the Federal Bureau of Investigation on behalf of Massachusetts law enforcement agencies, disaggregated by law enforcement agency on whose behalf the search was performed.³⁵

For each category of data and each law enforcement agency, the published information must specify the number of requests made or searches performed pursuant to a court order, the number of emergency requests made, or searches performed, and the reason for requesting the search, including, but not limited to, any underlying suspected crime.³⁶

c. Use of Facial Recognition After Police Reform

The Police Reform Law requires the RMV, MSP or FBI to run all law enforcement facial recognition searches. The Commission therefore invited Commissioners Colleen Ogilvie, Registrar of the RMV, and MSP Major Scott Range, who previously oversaw the Massachusetts Department of Homeland Security and Preparedness, to provide an overview on the systems and processes in place for their use of the technology on May 21, 2021.

According to Commissioners Ogilvie and Range, the Commonwealth operates one centrally controlled facial recognition database, which is used for fraud prevention by the RMV and investigations by law enforcement.³⁷ Only RMV personnel assigned to the RMV Enforcement Services Unit (civilian personnel) and MSP Troopers assigned to the State Police Fraud Identification Unit have access to this database. All MSP personnel are required to follow Department of State Police Policy and Procedure “Use of Facial Recognition Technology” when processing and fulfilling requests for searches.³⁸

Through a competitive bid process, the RMV contracted with Idemia, a French-based corporation that provides security services for both government and private sectors, for facial recognition services. The RMV’s database contains only images collected by the RMV or its partner AAA agencies, and its current gallery contains nearly six million images.

The RMV and AAA agencies collect and upload images multiple times a day, and the RMV then conducts searches of the existing gallery. This process includes a face verification, or 1-to-1 comparison, to ensure consistency between submitted materials attached to the same individual. It also includes face identification, or 1-to-many comparison, to uncover inconsistencies which could be symptomatic of fraud. The RMV reports that it searches nearly 6,000 images against the database daily and that it flags between 1,200 and 1,500 for manual review by RMV personnel.

³⁵ Id. at Section 26(d).

³⁶ Id.

³⁷ See footnote 22, *supra*.

³⁸ MSP’s Department of State Police Policy and Procedure “Use of Facial Recognition Technology” is included in Appendix H.

While it resolves most cases internally, the RMV forwards about 50 cases per day to the MSP to review for potential fraud. The MSP then advises the RMV on how to proceed – either by referring the case for a criminal investigation, creating an administrative case, or dismissing the potential match.

In addition to assisting the RMV with fraud investigations, the MSP assists other law enforcement agencies with requests for searches in criminal investigations. MSP personnel are assigned to the Commonwealth Fusion Center where they collect, log and evaluate requests from law enforcement agencies for facial recognition searches against the RMV database using the Idemia software. MSP reports that it does not utilize any other facial recognition database.

d. Facial Recognition Regulation by Massachusetts Municipalities

On July 9, 2021, Commissioner Kade Crockford provided the Commission with an overview of regulations passed by municipalities and other jurisdictions prohibiting or limiting the use of facial recognition and other biometric technologies. Commissioner Crockford also provided Commissioners with a memorandum outlining these regulations in more detail.

As of December 31, 2021, eight municipalities in the Commonwealth of Massachusetts have passed local ordinances regulating the use of facial recognition.³⁹ Many of these ordinances prohibit the municipal government, including any local police department, from obtaining, retaining, accessing, or using any face surveillance system or any information derived from a facial surveillance system.

Springfield's ordinance restricts municipal use of facial recognition technology until the city's police department puts forward rules governing the software that the council must then approve. Ordinances in Boston and Brookline explicitly prohibit the municipal government from entering into an agreement with or issuing a permit to a third party for the purpose of obtaining, retaining, possessing, accessing, or using any face surveillance system or information derived from a face surveillance system by or on behalf of the municipality or a municipal official. Northampton's ordinance prohibits any city official from expending city resources to obtain, retain, access, or use any face surveillance system.

e. Legislation in Other Jurisdictions

³⁹ City of Boston Municipal Code Section 16-62, Ordinance Banning Face Surveillance Technology in Boston; Town of Brookline Town By-Laws Article 8.39, Ban On Town Use Of Face Surveillance; Cambridge Code of Ordinances Section 2.128.075, Prohibition on City's Acquisition and/or Use of Face Recognition Technology; Easthampton City Ordinances Chapter 6, Section 6-22, Ban on Facial Recognition Surveillance Technology; Northampton Code of Ordinances, Chapter 290-1, Surveillance Systems; Somerville Code of Ordinances Section 9-25, Banning The Usage Of Facial Recognition Surveillance Technology; Springfield Code of Ordinances Chapter 173, Facial Recognition Surveillance Technology; City of Worcester Chapter 2 of the Revised Ordinances of 2008, Section 41, Ban on Facial Recognition Technology.

As of December 31, 2021, nine other states have passed laws that limit or regulate the use of facial recognition: California, Maine, Minnesota, New Hampshire, New York, Oregon, Utah, Vermont, Virginia, and Washington.

Vermont⁴⁰ and Virginia⁴¹ enacted broad moratoria on law enforcement use of facial recognition that will remain in place until the legislature affirmatively authorizes use of the technology. California,⁴² New Hampshire,⁴³ and Oregon⁴⁴ enacted laws focused on limiting law enforcement use of facial recognition technology in connection with body-worn cameras. New York⁴⁵ and Minnesota⁴⁶ enacted laws restricting the use of facial recognition in other limited areas. Utah, Washington, and Maine enacted the broadest legislation restricting the use of this technology.

i. **Utah**

⁴⁰ 2019 Vermont Senate Bill No. 124, Vermont 2019-2020 Legislative Session. <https://legislature.vermont.gov/bill/status/2020/S.124>. This legislation contains an exception for permitted law enforcement use of facial recognition with drones under 20 V.S.A. § 4622. Subsequent law created another exception to the moratorium for law enforcement use of facial recognition in cases involving the sexual exploitation of children. Vt. Stat. Ann. tit. THIRTEEN, Pt. 1, Ch. 64, Refs & Annos (West) <https://legislature.vermont.gov/bill/status/2022/H.195>.

⁴¹ 2020 Virginia House Bill No. 2031, Virginia 2021 Regular Session, 2020 Virginia House Bill No. 2031, Virginia 2021 Regular Session. <https://lis.virginia.gov/cgi-bin/legp604.exe?212+sum+HB2031>. The moratorium does not cover “commercial air service airports.”

⁴² California enacted a temporary moratorium on the use of facial recognition and other biometric surveillance in connection with body-worn cameras, including footage, and mobile devices that expires on January 1, 2023. Cal. Penal Code § 832.19. https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.

⁴³ New Hampshire law prohibits the use of video content analytics, including facial recognition technology, on recordings from body-worn cameras, and prohibits the use of facial recognition when issuing drivers’ licenses. N.H. Rev. Stat. Ann. § 105-D:2. <http://www.gencourt.state.nh.us/rsa/html/vii/105-d/105-d-mrg.htm>; N.H. Rev. Stat. Ann. § 263:40-b. <http://www.gencourt.state.nh.us/rsa/html/XXI/263/263-mrg.htm>.

⁴⁴ Oregon laws prohibit the use of facial recognition or other biometric-matching technology to analyze recordings obtained through the use of body-worn cameras. Or. Rev. Stat. Ann. § 133.741. <https://www.oregonlaws.org/ors/133.741>

⁴⁵ New York enacted a moratorium on the use of biometric identification technologies, including facial recognition, in schools, which is set to expire on July 1, 2022, or when the commissioner of education authorizes such purchase or utilization following the conditions laid out in the statute, whichever occurs later. NY LEGIS 349 (2020), 2020 Sess. Law News of N.Y. Ch. 349 (A. 6787-D) (McKINNEY’S). <https://nyassembly.gov/leg/?bn=S05140&term=2019>

⁴⁶ Minnesota prohibits law enforcement from deploying an unmanned aerial vehicle with facial recognition or other biometric-matching technology unless expressly authorized by a warrant. Minn. Stat. Ann. § 626.19. <https://www.revisor.mn.gov/statutes/cite/626.19>

Utah became one of the first states to enact comprehensive legislation regulating the use of facial recognition technology.⁴⁷ This law, effective May 5, 2021, designates the Department of Public Safety as the only state government entity authorized to use a facial recognition system to conduct a facial recognition comparison on an image database that is maintained by or shared with the department. Law enforcement may request the department run a facial recognition search for the purpose of investigating a felony, violent crime or threat to someone's life, or to identify an individual who is deceased, incapacitated, or at risk and otherwise unable to provide his or her identity.⁴⁸ Such request must be in writing and, if for the purpose of investigating a crime, supported by a statement of the specific crime and factual narrative to support that there is a fair probability that the individual who is the subject of the request is connected to the crime. Searches must go through at least three levels of review before being reported by the department as a probable match.

The law sets forth annual reporting requirements for government entities using facial recognition, which includes disclosing: (i) the different types of crimes for which the department received a request; (ii) how many requests the department received for each type of crime; (iii) the number of probable matches the department provided in response to each request; and (iv) the image source from which the department made each match.

Additionally, the law requires a government entity to notify an individual, when capturing an image of that individual, that said image may be used in conjunction with facial recognition technology. It also sets forth a procedure for the review and approval of other governmental agencies' use of facial recognition software, which includes notice and public input requirements.

ii. **Washington**

Washington's law,⁴⁹ effective July 2021, includes comprehensive regulations authorizing and regulating the use of facial recognition and prohibits governmental agencies from using facial recognition systems in certain circumstances, including:

- i. engaging in real-time surveillance absent a warrant, exigent circumstances, or a court order authorizing such use for locating and identifying a missing person;
- ii. using the technology on an individual based on certain protected characteristics (e.g., religious, political, or social views or activities, participation in a particular noncriminal organization or lawful event, or actual or perceived race, ethnicity, citizenship, place of

⁴⁷ While the Commission did not specifically discuss Utah's legislation in its deliberations, it makes note of this law, which was enacted in May of 2021. Utah Code Annotated §77-23e-104.

https://le.utah.gov/xcode/Title77/Chapter23E/77-23e-S104.html?v=C77-23e-S104_2021050520210505

⁴⁸ This law also specifically prohibits government entities from using facial recognition for a civil immigration violation.

⁴⁹ Wash. Rev. Code Ann. § 43.386.000 et. seq. (West).

<https://app.leg.wa.gov/billsummary?BillNumber=6280&Year=2019&Initiative=false>

- origin, immigration status, age, disability, gender, gender identity, and sexual orientation);
- iii. creating a record describing an individual’s exercise of their freedom of speech, association, or religion;
- iv. using search results as the sole basis to establish probable cause in a criminal investigation;
- v. identifying an individual based on a sketch or manually produced image; and
- vi. substantively manipulating an image for use in a facial recognition system in a manner not consistent with the vendor’s intended use and training.

The law also creates a process, including issuing an accountability report and holding public hearings, that agencies must follow when they intend to use facial recognition in a permitted application. The technology must be tested in “operational conditions” before use and, if the specific use could produce “legal effects concerning individuals,” those decisions must be subject to “meaningful human review.” The law mandates specific training requirements for employees who use facial recognition and requires vendors with government contracts to create an Application Programming Interface (API) that enables independent audits and accuracy tests. Additionally, prosecutors must disclose the use of facial recognition technology in criminal investigations in a timely manner before trial.

ii. Maine

Maine’s law, effective October 1, 2021, contains the broadest restriction on the use of facial recognition thus far in the nation.⁵⁰ The law establishes a general rule that public agencies and officials in Maine may not: (i) obtain, retain, possess, access, request, or use a facial recognition system or information derived from a search of a facial recognition system; (ii) enter into an agreement with a third-party to obtain, retain, possess, access or use a facial recognition system or information derived from a search of a facial recognition system; or (iii) issue a permit or enter into any other agreement that authorizes a third-party to obtain, retain, possess, access or use a facial recognition system or information derived from a search of a facial recognition system.

Maine law does preserve the ability of the Maine Bureau of Motor Vehicles to use facial recognition to identify and investigate fraud in the licensing process.⁵¹ The general prohibition also does not apply in the following circumstances:

- i. using facial recognition technology that analyzes the eye’s iris in a regional jail or county jail;
- ii. using evidence that may have been generated from a search of a facial recognition system related to an investigation of a specific crime;

⁵⁰ Sec. 1. 25 MRSA Pt. 14, Ch. 701, §6001. [getPDF.asp \(mainelegislature.org\)](https://www.mainelegislature.org/getPDF.asp)

⁵¹ Me. Rev. Stat. tit. 29-A, § 1401. <http://legislature.maine.gov/statutes/29-A/title29-Asec1401.html>

- iii. obtaining or possessing for evidentiary purposes an electronic device that performs facial recognition for the sole purpose of user authentication;
- iv. using social media or communications software or applications to communicate with the public as long as such use does not include the affirmative use of facial recognition;
- v. using automated redaction software without facial recognition capabilities;
- vi. performing duties required by the National Child Search Assistance Act of 1990; and
- vii. using facial recognition on an electronic device owned by a public employee or public official for that person's personal use for the sole purpose of user authentication.

Additionally, Maine's law establishes three investigatory and public safety exceptions to the general prohibition, including:

- i. when there is probable cause to believe that an unidentified individual in an image has committed the serious crime (i.e., a crime punishable by a term of imprisonment of one year or more, or a Class D and Class E crime under Maine law);⁵²
- ii. assisting in the identification of a person who is deceased or believed to be deceased; and
- iii. assisting in the identification of a missing or endangered person.

The Bureau of Motor Vehicles is responsible for conducting all in-state search requests, while the Maine State Police is responsible for all out-of-state search requests made to the FBI or another agency. A government agency may request an out-of-state search directly only on an emergency basis and must file disclosure documentation detailing the emergency search with the Maine State Police as soon as practicable.⁵³

Maine's law requires the Maine State Police and the Bureau of Motor Vehicles to track, as public records, all requests for searches of facial recognition systems, anonymized and containing: the date of the search request; the name of the public employee or public official who made the request; the name of the department for which the employee or official works; the databases searched; the statutory offense under investigation; and the race and sex of the person under investigation.⁵⁴

Any facial recognition data collected or derived in violation of the law is considered unlawfully obtained and, except as otherwise provided by law, deleted upon discovery. Such data

⁵² Maine's law also specifically provides that facial recognition data does not, without other evidence, establish probable cause justifying arrest, search, or seizure.

⁵³ The Bureau of Motor Vehicles may request a search of a facial recognition system from an out-of-state state agency or the FBI for fraud prevention or investigation purposes.

⁵⁴ Maine's law provides a limited exception to the public nature of these logs to the extent the Intelligence and Investigative Record Information Act applies. Me. Rev. Stat. tit. 1, chap.13.
<https://www.mainelegislature.org/legis/statutes/1/title1ch13sec0.html>

is inadmissible as evidence in any proceeding and any person injured or aggrieved by a violation of the law may file a lawsuit against the department, public employee, or public official having possession, custody, or control. The law also provides for disciplinary actions against public employees or officials who, in the performance of their official duties, violate the law.

VI. Advantages and Disadvantages of Government Use of Facial Recognition

a. Utility of Facial Recognition

The Commission reviewed testimony from law enforcement professionals, investigative organizations and facial recognition software companies on the importance and utility of facial recognition in promoting public safety. Proponents state that the benefits of the technology, especially its application in identifying suspects and victims of serious crime, outweigh concerns raised.⁵⁵ MCCA noted in its 2021 Facial Recognition Working Group's report:

The 21st century offers law enforcement an unprecedented opportunity to embrace advanced technologies to keep our communities safe. One of the most valuable of these technologies is facial recognition technology (FRT). FRT has an unprecedented ability to combat criminal activity, identify persons of interest, develop actionable leads, and close cases faster than ever before. Perhaps most importantly, the law enforcement agencies which have embraced this technology have proven its capability of assisting with the ultimate goal of keeping our communities safe...Technology has an ever-increasing impact on our lives. As such, it is critical that law enforcement also have access to and develop programs that leverage these advanced technologies to combat the criminal element.

Numerous law enforcement and prosecuting agencies, in their responses to the Initial Survey, asserted that facial recognition "is a necessary tool for law enforcement which has led to many identifications of suspects that would not have been identified otherwise," and emphasized that "[i]t helps build towards probable cause, but it is not probable cause itself. You need to corroborate the match and have other evidence to support the match as well."

The Suffolk County District Attorney's Office stated in its response:

While public safety and privacy interests seem to be often in conflict in this space, the true value of these tools and their contribution to public safety and public health seldom get adequate representation. There are several critical areas that facial recognition tools tip heavily to the public safety side of the spectrum that should be mentioned; they include counterterrorism and critical incident response,

⁵⁵ Digital Fourth, however, noted in testimony submitted to the Commission: "We have worked extensively on passing facial recognition bans in Cambridge, Somerville, Brookline and now Boston, and we observe that none of these communities have faced crime waves as a result. Refraining from using this biased technology may in fact increase the effectiveness of policing, by preventing police from wasting time chasing falsely identified leads."

transportation security, and investigations into missing and exploited children.⁵⁶

Proponents of facial recognition also argue that many concerns stem from public misconception about outdated and lower-performing technology. They point to a recent study conducted by the National Institute of Standards and Technology (“NIST”), a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce, as support.⁵⁷ Rank One Computing noted in testimony submitted to the Commission, “[t]he 2019 NIST Demographic Effects report found that top-tier face recognition technologies had ‘undetectable’ differences in accuracy across racial groups...Government applications use top-tier face recognition algorithms from NEC, Idemia and Rank One Computing, not the lower-performing submissions.”⁵⁸

Citing this report, MCCA concluded that “the soundest alternative to banning FRT is adopting appropriate regulations mandating that only thoroughly-trained image analysis algorithms, meeting certain accuracy thresholds be utilized by law enforcement and that assessment by independent testers be funded to ensure continuous improvement of the technology so that only the most effective tools are deployed in the field.”⁵⁹

b. Concerns with Facial Recognition

The Commission received a significant volume of testimony from politicians, academics, reform advocates, scientists, and other individuals highlighting concerns with the unregulated use of facial recognition technology by the government. These included, but were not limited to, concerns over accuracy, constitutional infirmities, due process violations, and invasions of

⁵⁶ Clearview AI founder and CEO Hoan Ton That stated in written testimony submitted to the Commission that “[a]ny ban on facial recognition will be devastating for victims of child rape and human trafficking. Likewise, limiting the dataset law enforcement can use to DMV photos or mugshots will prevent victims of child exploitation from being rescued, as children are not in DMV databases.”

⁵⁷ Patrick Grother, Mei Ngan, Kayee Hanaoka, National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (December 19, 2019), <https://doi.org/10.6028/NIST.IR.8280>;

⁵⁸ The ACLU of Massachusetts, however, noted in testimony submitted to the Commission: “Notably, the federal government testing mentioned...was run in a quality-controlled research setting using standardized photographs, such as police mugshots and visa application portraits — and it still showed major inaccuracies. Using these algorithms to identify faces in ‘wild’ photographs taken from surveillance footage will only worsen demographic disparities because those photos are often very low-quality.”

⁵⁹ The Commission also received written testimony from Massachusetts Chiefs of Police Association (MCOPA) stating: “It is important to remember that facial recognition has been utilized for as long as crimes have been investigated. Law enforcement often relies on human witnesses to match images with either photographs or in-person lineups. These applications of eyewitness facial recognition have been proven to be incredibly susceptible to bias particularly when the process is flawed by human error. It seems, when applicable, the use of a digital algorithmic system, which can be administered, restricted, tested, audited, and improved, is far superior to the use of visually based facial recognition.”

privacy.

i. Accuracy Concerns

The Commission noted general concerns about the accuracy of facial recognition technology as well as specific concerns relating to accuracy rates based on race and gender. With respect to general accuracy concerns, Commissioner Learned-Miller and his colleagues cautioned:

Since a particular person's appearance may vary significantly from one time to another, two faceprints of the same person are rarely exactly the same... Conversely, two different people with similar superficial features (say, a certain style of beard), or whose photos were taken under similar conditions may, in some cases, have nearly identical faceprints... The inability for any technology to generate a unique faceprint for each individual is at the heart of many face recognition system errors.

The Project on Government Oversight noted:

Image quality can [] significantly impact accuracy of matches... Bad lighting, indirect angles, distance, poor camera quality, and low image resolution all make misidentifications more likely. These poor image conditions are more common when photos and videos are taken in public, such as with a CCTV camera. But these low-quality images often serve as probe images for face recognition scans, without due consideration for their diminished utility.⁶⁰

Commissioner Ogilvie, in her presentation to the Commission on behalf of the RMV, noted that an "average of 20% (1,200 – 1,500 records) [of searches on the RMV's database are typically] flagged as a potential match for manual review." Other Commissioners and members of the public claim that this suggests a lack of confidence in accuracy.

In addition to general accuracy concerns, the Commission received testimony and research finding that all facial recognition software, even "top-tier technologies," have a lower accuracy rate for certain demographics including persons of certain races and genders.⁶¹ The Project on Government Oversight continued:

⁶⁰ The MCCA agreed: "In reality, no biometric system is this perfect. Changes in pose, illumination, and expression, among other factors, can reduce the match score generated for a true match pair, while twins and other "lookalikes" can lead to non-match pairs with high scores..." Major Cities Chiefs of Police; 2021 Facial Recognition Working Group, Facial Recognition Technology in Modern Policing: Recommendations and Considerations (2021).

⁶¹ The Pirate Party noted in testimony submitted to the Commission: "Facial recognition software relies on machine learning systems to find matches and make connections between the faces given to them and the faces they analyzed in their training data. When that training data is biased, as it often is, then the results will be biased."

The quality of face recognition algorithms can vary significantly. Notably, many algorithms misidentify women and people of color at a higher rate than other people. Studies by the National Institute of Standards and Technology; the Massachusetts Institute of Technology, Microsoft, and AI Now Institute researchers; the American Civil Liberties Union; and an FBI expert all concluded that face recognition systems misidentify women and people of color more frequently. Failure to recognize the significance of this problem—and account for it in selection and review of software, training, and auditing—will undermine investigations and seriously harm civil rights.⁶²

Reform advocates cited two main studies in support of their assertion that facial recognition is less accurate on women and persons of color. The first, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” led by Joy Buolamwini of the Massachusetts Institute of Technology and Timnit Gebru of Microsoft Research, found that facial surveillance technology exhibits gender and racial bias, with some algorithm failure rates erring up to one third of all cases evaluating the faces of darker skinned females.

The second was NIST’s 2019 study, “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,” led by Patrick Grother, Mei Ngan, Kayee Hanaoka, finding that most face recognition algorithms exhibit demographic differentials, particularly for women, children, elderly, and persons of color.⁶³ For one-to-one matching, NIST saw higher rates of false positives for Asian and African American faces relative to images of Caucasians. The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm. For one-to-many matching, NIST saw higher rates of false positives for African American females. The study found both “false positives” in which an individual is mistakenly identified, and “false negatives” where the algorithm fails to accurately match a face to a specific person in a database.

The NAACP New England Area Conference and GLAD cited these studies in testimony submitted to the Commission and urged that this technology, which is less accurate for persons of color and LGBTQ+ individuals (groups who already experience increased incidents of discrimination and over-policing) should be prohibited or, at the very least, highly regulated and reported.⁶⁴ Furthermore, with respect to gender, GLAD noted that facial recognition software

⁶² MCCA contest these findings, arguing that: “The perception of facial recognition being biased began with early versions of the technology showing inconsistent accuracy rates across different demographics such as age, gender, and skin color... Today, the general accuracy of facial recognition technology has improved substantially and like most technology, rapidly continues to more so every year.”

⁶³ Notably, proponents of facial recognition cite this same NIST report to show that “[t]he most accurate identification algorithms have ‘undetectable’ differences between demographic groups.”

⁶⁴ The NAACP New England Area Conference stated that “[t]he use of biometric recognition technologies, especially facial recognition, directly undermines racial justice. The government should not be allowed to use technology that disproportionately harms Black communities that already suffer from over-policing.”

only sorts faces as ‘male’ and ‘female,’ although there is a much wider spectrum of genders, gender identities and gender expression, and “routinely fails to correctly identify transgender people.”⁶⁵

The Commission noted that, even if accuracy rates are relatively high for a particular facial recognition software, and have reportedly successfully generated investigative leads in various cases, an inaccurate result may lead to a significant and unacceptable miscarriage of justice, including unnecessary police interactions and wrongful detention, arrest, and incarceration.⁶⁶ The Commission heard testimony from Robert Williams, who was arrested based on an inaccurate facial recognition search in front of his neighbors, wife, and young children. Mr. Williams testified that this wrongful arrest caused him severe and ongoing trauma and has had lasting effects on his health, family, employment and finances.

ii. Constitutional/Due Process Concerns

Groups also expressed serious concerns about constitutional and due process violations relating to the use of facial recognition and the notification of subjects of a facial recognition search. Advocates for reform claim that a facial recognition search amounts to an unreasonable search and seizure in violation of the U.S. Constitution.⁶⁷ Supporters of facial recognition, however, disagree, arguing that still-developing case law means that this issue is not settled. Advocates for reform believe that the existing standard for law enforcement use of facial recognition as enacted in the Police Reform Law, namely, pursuant to a court order “based upon specific and articulable facts” is insufficient and must be replaced with a probable cause standard to meet constitutional requirements.

The Project on Government Oversight noted in testimony submitted to the Commission:

⁶⁵ GLAD further noted: “A review of four facial recognition programs concluded that the software failed to correctly identify the gender of transgender men in over one-third of cases, whereas the programs correctly identified other men almost all of the time. Further, facial recognition algorithms universally fail to correctly identify the gender of individuals who identify neither as male or female - an error rate of 100%.” *Citing* Lisa Marshall, Facial recognition software has a gender problem, UNIV. CO. BOULDER (October 8, 2019), <https://www.colorado.edu/today/2019/10/08/facial-recognition-software-has-gender-problem>.

⁶⁶ Commissioner Brooks stated that facial recognition technology in and of itself does not lead to a miscarriage of justice. Rather, he asserts, the only way a miscarriage of justice occurs is if law enforcement takes an unsubstantiated lead and makes an arrest without corroboration.

Other Commissioners pointed to the proper use of facial recognition as an investigative tool in criminal investigations in many cases. Specifically, Commissioners O’Keefe and Woodward noted that, from October 8, 2016, to October 8, 2019, the NYPD conducted 22,069 facial recognition searches with no cases of false arrests reported.

⁶⁷ The U.S. Constitution provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const., amend. IV.

Requiring that law enforcement demonstrate probable cause... is a critical safeguard for preventing abuse. The primary police use for face recognition is to scan photographs of individuals taken during commission of a crime; demonstrating probable cause in such scenarios should not be an onerous burden for supporting legitimate law enforcement goals.

Digital Fourth reiterated this sentiment in its testimony submitted to the Commission, asserting that “probable cause warrants matter...because they require a court to provide independent review, to make sure that the government is only searching or seizing if they already have good reason to suspect that [a particular person is] involved in an actual crime.”

Advocates for reform also believe that facial recognition should be limited to use for serious crimes only. The ACLU noted that “[g]overnment use of facial recognition technology is extremely privacy invasive, and therefore should not be used to attempt to identify a person for minor offenses such as trespassing, shoplifting, or jaywalking. Facial recognition searches should only be authorized in the most serious types of criminal investigations, investigations of serious violent felonies.” Testimony from the League of Women Voters pointed to similar restrictions placed on the use of wiretap technology as support for this measure.

Advocates for reform also asserted that regulations must ensure that government entities inform subjects of a facial recognition search of that search in a timely manner. This is especially necessary to provide defendants due process under the law. The ACLU noted:

[E]xisting law does not provide any due process protections for criminal defendants that have been subject to the use of facial recognition systems. The law should be explicit on this point to ensure prosecutors are not intentionally or unintentionally violating people’s constitutional rights to a fair trial by withholding information about the use of technology that effectively constitutes a digital witness.

The Project on Government Oversight highlighted the importance of this information to a defendant’s investigation, preparation, and defense of their case, explaining:

Defendants have a vested interest in reviewing a variety of factors, such as algorithm quality, the software settings police used, and whether any other potential matches were discovered or investigated, that could provide exculpatory or mitigating evidence. Guaranteeing access to this information is not only critical for due process rights but also acts as an important safeguard to deter corner cutting and sloppy use of face recognition during investigations.

Commissioner Maurice Dyson, calling for centralized, statewide control of all facial recognition usage, noted, “It is intended that by centralizing police use of facial recognition in one agency, it will facilitate simpler auditing and oversight, thereby strengthening civil rights,

protecting racial justice, guarding against abuse and misuse, and protecting the integrity of the criminal legal system.”

Lastly, several Commissioners, advocacy groups, and individuals advocated for stronger enforcement provisions to ensure public officials’ compliance with restrictions and regulations on the use of facial recognition. Suggested provisions included excluding any facial recognition data collected or derived in violation of the law as evidence in any proceeding, providing administrative penalties, and establishing an individual cause of action by persons aggrieved by a violation of the law.

iii. Privacy Concerns

Several Commissioners and many other individuals and organizations raised serious concerns over the potential for facial recognition to be used for general surveillance in public spaces without any exigent safety circumstances. The Electronic Frontier Foundation noted in testimony submitted to the Commission, “[f]ace surveillance is a particularly pernicious form of surveillance because of the scope at which it amplifies already existing bias and the scale at which it provides for the persistent, untiring, and covert monitoring of our actions and associations.”

The ACLU warned that this “technology can facilitate a massive surveillance infrastructure where everyone is identified, wherever they go, all the time...People in Massachusetts should be able to walk around their communities, visit friends and family, seek medical treatment, go to church, and attend political events without worrying that the government is secretly keeping tabs on their every movement, habit, and association.”

VII. Deliberations

Following the testimony, presentations, research, and discussions noted above, the Commission considered a variety of possible recommendation topics suggested by both the public and Commissioners. The Commission held detailed deliberations over multiple sessions focusing on the following topics:

1. Law Enforcement Use of FR Technology
 - a. Application:
 - i. Should other applications or uses of facial recognition technology beyond image matching be prohibited or regulated (i.e., surveillance, tracking, emotional recognition)?
 - b. System:
 - i. Should other facial recognition systems and databases, including private systems, be permitted for use by law enforcement in the Commonwealth instead of or in addition to the RMV’s database?
 - c. Accuracy:
 - i. What minimum thresholds and standards should the legislature impose with respect to image quality and comparison accuracy of facial

- recognition systems used by law enforcement in the Commonwealth (NIST score, size and diversity of data sets, confidence thresholds, human review, etc.)?
- ii. Should a government office or department be tasked with promulgating further regulations on accuracy and updating those regulations as technology improves and circumstances change? If so, who (i.e., EOTSS, AG)?
- d. Usage:
 - i. In what circumstances should law enforcement agencies be able to use facial recognition technology (i.e., violent crimes, identity fraud, exigent circumstances)?
 - ii. Should the legislature change the existing legal standard for law enforcement use of facial recognition? If so, to what (i.e., reasonable suspicion, probable cause, exigent circumstances)?
 - iii. Should judicial review and approval be required for each request to use facial recognition? What should that process look like?
 - iv. Should there be any exceptions (i.e., exigent circumstances, identifying a deceased person)? What should that process look like?
 - v. Should restrictions be imposed on when, how, and how long images used in a facial recognition search may be stored, and under what conditions stored images can be further used?
- e. Control:
 - i. Should law enforcement use of facial recognition be centralized within one office or department? If so, with whom?
 - ii. What should the process look like for law enforcement agencies to request that the centralized office conduct a facial recognition search?
- f. Oversight & Training:
 - i. What training should be required on the use of facial recognition systems and review and interpretation of search results?
 - ii. What oversight should be required by the legislature (i.e., collection of certain data, regular audits, specific reporting requirements)?
 - iii. Should a government office or department be tasked with promulgating further regulations on training and oversight and, if so, who?
 - iv. What government office or department should be entrusted with oversight?
- g. Legal Protections:
 - i. What standards and protocols should be in place relating to privacy, civil rights, due process, and other legal protections in connection with the use of facial recognition technology?
 - ii. When, how, and under what circumstances should the subject of a facial recognition search be notified?
- 2. Other Government Use of FR Technology
 - a. Should other government use of FR technology be similarly regulated (i.e., schools, airports)?

- b. Should other government use of FR technology be prohibited until it can be investigated further?

VIII. Recommendations

After several lengthy and detailed deliberation sessions, a majority of the Commission found that facial recognition can be used in limited, tightly regulated circumstances to advance legitimate criminal investigations.⁶⁸

Additionally, Commissioners expressed marked concern over other government use of facial recognition, including in schools and airport security. However, the Commission determined that it needed to devote significant attention to law enforcement use of facial recognition and the possible further regulation thereof as a threshold matter. The Commission is, therefore, not in a position to recommend specific regulations on other government use at this time. It strongly recommends further consideration of this area following the implementation of the law enforcement-focused recommendations contained in this report.

Accordingly, the Commission makes the following formal recommendations to the General Court based on its study of government use of facial recognition in the Commonwealth:

1. The Commission recommends that the Legislature build on the standards and regulations first enacted in the Police Reform Law with respect to law enforcement use of facial recognition. More specifically, the Commission recommends that the Legislature amend Section 26 of Police Reform Law to clarify that a law enforcement agency or law enforcement officer, as defined in Section 30 of Police Reform Law, is prohibited from acquiring, possessing, accessing, using, assisting with the use of or providing resources for the development or use of any facial recognition system, or to enter into a contract or make a request to any third party, including any federal agency, for the purpose of acquiring, possessing, accessing, or using information derived from a facial recognition system absent express statutory authorization.
2. The Commission recommends the exclusion of any information obtained in violation of facial recognition regulations from any criminal, civil, administrative, or other proceeding.
3. The Commission recommends that legislation specify that only the MSP is authorized to perform a facial recognition search or request the FBI to perform such a search in criminal investigations.

⁶⁸ For example, Commissioner Conley stated in written testimony submitted on behalf of MCOPA: “It is our position that this technology should remain available to law enforcement, however, we agree that reasonable regulations should be adopted to detect abuse and ensure public transparency.”

4. The Commission recommends that the only facial recognition software the MSP may access is either the existing software used by the RMV and FBI or facial recognition technology software approved by the Executive Office of Technology Services and Security (“EOTSS”), which may only be approved following a public hearing on the proposed software.
5. The Commission recommends that legislation specify that facial recognition technology should only be used in investigations of felonies.
6. The Commission recommends that a search only be permitted pursuant to a warrant issued by a judge based on probable cause that an unidentified or unconfirmed individual in an image has committed a felony.⁶⁹
7. The Commission, however, also recognizes the need for law enforcement professionals to be able to respond to emergency situations, and therefore recommends that the MSP be allowed to conduct a facial recognition search without a warrant if the law enforcement agency making the request reasonably believes that an emergency involving immediate danger of death or serious physical injury to any individual or group of people requires the performance of a facial recognition search without delay. In these situations, the Commission recommends that the law stipulate that the requesting agency make the search in writing, narrowly tailored to address the specific emergency, and that the agency document the factual basis for the emergency as discussed further below.
8. The Commission recommends creating an exception to allow a facial recognition search without a warrant or emergency requirement to identify a deceased person.
9. The Commission recommends the Legislature prohibit law enforcement use of emotion recognition, surveillance⁷⁰ and tracking, which are nascent, overreaching technologies with low reliability.
10. The Commission recommends that there be one state-level facial recognition operations group within the MSP charged with: (i) receiving and evaluating law enforcement requests for facial recognition searches; (ii) performing facial recognition searches; (iii) reporting results; and (iv) recording relevant

⁶⁹ 81% of police departments who responded to the Commission’s Initial Survey reported that they do not use face recognition technology and have no plans to use it. Therefore, the Commission finds that limiting the use of facial recognition to address due process and constitutionality concerns will not unduly burden criminal investigations.

⁷⁰ However, this recommendation does not prohibit law enforcement from taking a still image from surveillance footage and running that through facial recognition, provided the search otherwise meets the requirements of the law.

data. The Commission finds that the centralization⁷¹ and standardization⁷² of this process will promote efficiency, ensure consistency, improve training and foster more accountability and transparency.

11. The Commission recommends that, in the case of an emergency search, the law enforcement agency making the request file with the superior court a signed, sworn statement made by a supervisory official of a rank designated by the head of the agency setting forth the grounds for the emergency search within 48 hours, unless the superior court issues an order for delayed notice detailing the ongoing nature of the emergency and the continuing and immediate threat to public safety.
12. The Commission further recommends that the legislation specify that after a defendant is charged with a crime, the attorney general or district attorney notify the defendant, pursuant to Rule 14 of the Massachusetts Rules of Criminal Procedure, that they were identified using the technology. This notice allows the defendant to challenge potential misidentification resulting from the use of the technology, bring a motion to suppress facial recognition identification based on law enforcement's use of the technology in violation of the law, or otherwise use this information in the defendant's defense of the case.
13. With respect to reporting, the Commission recommends that the MSP document each use of facial recognition and report this information quarterly to EOPSS. Reported information should include, but not be limited to: the date and time of the search; the specific criminal offense(s) under investigation; the system used for the search; the number of matched individuals returned, if any; the name and position of the requesting individual and employing law enforcement agency; a copy of the warrant, or if no warrant exists, a copy of the written emergency request; and data detailing the individual characteristics included in the facial recognition request, including the presumed race and gender of the person in the probe image(s), as assessed by the MSP officer conducting the search. EOPSS will report this information, along with certain aggregated data, on its website annually in accordance with existing requirements contained in Section 26 of the Police Reform Law.

⁷¹ The ACLU noted in testimony submitted to the Commission: "Chaotic and decentralized implementation of facial recognition technology is bad from both a prosecutorial and a civil rights perspective, and makes effective accountability, transparency, and oversight nearly impossible. The law must therefore centralize government use of facial recognition for investigative purposes and limit the agencies that can possess the technology."

⁷² The Commission also discussed recommending that all law enforcement facial recognition search requests and results be submitted and reported through a central portal, via a secure web interface, to further promote efficiency and standardization. However, the Commission ultimately decided to leave the logistics of its system to the MSP, with input and assistance from EOPSS and EOTSS.

The Commission finds that these changes, if adopted by the Legislature, will set appropriate guidelines and restrictions on law enforcement's use of facial recognition technology while acknowledging the potential benefits improved facial recognition technology have for public safety.

Special Commission to Evaluate Government Use of Facial Recognition Technology in the Commonwealth

Appendices

Appendix A:	Commissioner Vote Record on Final Report
Appendix B:	Letter from Supreme Judicial Court Chief Justice Budd
Appendix C:	Meeting Minutes
Appendix D:	Initial Survey Template
Appendix E:	Summary of Initial Survey Responses
Appendix F:	Follow-Up Survey Template
Appendix G:	Follow-Up Survey Responses
Appendix H:	Department of State Police Policy and Procedure “Use of Facial Recognition Technology

Appendix A
Commissioner Vote Record on Final Report

Special Commission on Facial Recognition
Commissioner Vote Record on Final Report

ASSENT

Chair Day
Chair Eldridge
Commissioner Rogers
Commissioner Hartzog
Commissioner Gomez
Commissioner Creem
Commissioner Dyson
Commissioner Cordy
Commissioner Rebello-Pradas
Commissioner Crockford
Commissioner Spurlock
Commissioner Nkonde
Commissioner Cyr
Commissioner Learned-Miller
Commissioner Verma

DISSENT

Commissioner Woodward
Commissioner Brooks
Commissioner Conley
Commissioner O'Keefe

ABSTAIN

Commissioner Farnsworth
Commissioner Ogilvie

Appendix B

Letter from Supreme Judicial Court Chief Justice Budd



**Supreme Judicial Court
John Adams Courthouse
One Pemberton Square, Suite 2500
Boston, Massachusetts 02108**

Kimberly S. Budd
Chief Justice

May 4, 2021

BY EMAIL

Honorable Michael S. Day, Co-Chair
State Representative
Thirty-First Middlesex
Special Legislative Commission
State House
24 Beacon Street, Room 136
Boston, MA. 02133
michael.day@mahouse.gov

Honorable James B. Eldridge, Co-Chair
Senator
Special Legislative Commission
State House
24 Beacon Street, Room 511-C
Boston, MA. 02133
james.eldridge@masenate.gov

RE: Commissions, St. 2020, Chapter 253

Dear Chairs Day and Eldridge:

As you may know, the Code of Judicial Conduct (Code) governs judges' ethical obligations, and it includes a rule that addresses judges' appointments to governmental positions. (Code of Judicial Conduct, Rule 3.4). Given that the Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth, St. 2020, Chapter 253, contains provisions regarding my action with respect to several Commissions, I sought guidance from our Committee on Judicial Ethics on whether the Code would impose any limitations or restrictions on my ability to serve (or appoint or designate someone to serve) on those Commissions (i.e. the commission to review and make recommendations with regard to correction officers and juvenile detention officers established under Section 103; the law enforcement body camera task force established under Section 104; and the Facial Recognition Commission established under Section 105). I recently received a response to my request for guidance and I regret to inform you that I am unable to act in any capacity with respect to these Commissions.

The Committee found that because the core work of the above-referenced Commissions is not sufficiently related to the work of the courts (i.e. there is not a direct nexus between the mandates of the Commissions and how the courts go about their business), the Code does not permit me to serve, or to designate or appoint others to serve on them. The Committee noted that it is likely that some of the work of the commissions could become the subject of future litigation, which would raise concerns about judicial independence. Further, the Committee advised me that the act of designating or appointing someone to serve on a governmental commission is itself a form of participation because it would involve me in the process of establishing the Commissions.

I do want to point out that although I may not make appointments myself, there is nothing to prevent a non-judge public official from appointing retired judges to serve on the Commissions (retired judges are not bound by the obligations of the Code). I am sorry that I am unable to assist you with the work of these Commissions, but I hope you understand; the rules in the Code are protective of the separation of powers demanded by article 30 of the Massachusetts Declaration of Rights. On matters related to the business of the courts, we are, of course, eager to help. I wish you and the Commission success in your work.

Sincerely,

A handwritten signature in dark ink, appearing to read "Kimberly S. Budd". The signature is fluid and cursive, with the first name "Kimberly" written in a larger, more prominent script than the last name "Budd".

Kimberly S. Budd

cc: Honorable Karen E. Spilka, Senate President
Honorable Ronald J. Mariano, Speaker of the House
Secretary Thomas A. Turco, III, Executive Office of Public Safety and Security
Secretary Curtis M. Wood, Executive Office of Technology Services and Security

Appendix C
Meeting Minutes

Special Commission on Facial Recognition Meeting Minutes
Friday, April 16, 2021 at 11:00 a.m.
(Virtual Meeting)

Agenda:

- I. Introduction of Commission Members and Staff
- II. Review of Legislative Commission Parameters and Adoption of Protocols
- III. Review and Discussion of Statutory Charge
- IV. Discussion of Topics for Future Meetings

Commissioners Present

Commissioner Rogers
Commissioner Woodward
Commissioner Hartzog
Commissioner Dyson
Senator Gomez- Lauren Matteoda on behalf of Senator Gomez
Commissioner Creem
Commissioner Brooks
Commissioner Cordy
Commissioner Rebello-Paradas
Commissioner Farnsworth
Commissioner Ogilvie
Commissioner Learned Miller
Commissioner Range
Commissioner Crockford
Commissioner Spurlock
Commissioner Verma
Commissioner O'Keefe
Commissioner Conley

Commissioners Absent

Commissioner NKonde

Representative Day confirmed with Seamus Corbett from the State House Legislative Information Services that the meeting was broadcasted on malegislature.gov and began the meeting on 4/16/21 at 11AM with a unanimous roll call.

Representative Day calls the first meeting of the Special Recognition on Facial Recognition to order at 11AM on 4/16/21.

Representative Day makes introductory remarks and introduces Senator Jamie Eldridge, co-chair of the Special Commission on Facial Recognition and the Joint Committee on the Judiciary.

Senator Eldridge makes introductory remarks.

Representative Day opens the meeting by asking Patrick Prendergast, Chief of Staff in the Office of Representative Day, the calling of the roll of the members.

Patrick Prendergast introduces the calling of the roll of the members.

Representative Day introduces his staff members who will be keeping minutes of these meetings and says they will be of service to all members.

Senator Eldridge introduces his staff members.

Representative Day notes the large size of the commission with upwards of 20 folks. Representative Day does a quick introduction, and states how impressed he is that each member has chosen to serve on the commission and is grateful for everyone's partnership considering their distinct backgrounds.

Representative Day introduces all commission members and provides brief biographies.

Representative Day says that agenda item 1 has been completed and notions to move into agenda item 2: the legislative commission parameters and the adoption of protocols, unless any commission members have anything they would like to add.

Commissioner Creem mentions that this is an impressive group and is honored to be a part of it. Commissioner Creem requests that a snapshot of the commission members and their biographies be shared with the group.

Representative Day notes that this has been completed and will be displayed when the commission website is shared. Representative Day continues to move into agenda item 2: The review of Legislative Commission Parameters and suggested adoption of protocols. Representative Day states that this is a special commission chaired by legislators who are the judiciary committee chairs in both the House and Senate and governed by the General Laws of the Commonwealth. While these rules and statutes empower us with broad authority to collect information in pursuit of meeting our charge, we are tasked with certain responsibilities as a commission. Chief among those is the requirement of Joint Rule 29 A, to maintain an open process which will provide members of the public with the opportunity to view, and sometimes participate, in our deliberations.

Representative Day asks Jacqui Manning, staff member in the Office of Representative Day, to share her screen and display Joint rule 29A.

Representative Day continues by mentioning that today's meeting has been noticed on the State Legislature website and is also being livestreamed there. Representative Day states that he looks forward to when the commission can meet in person, but that virtual meetings provide an opportunity for us to record our meetings. Representative believes that recording will prove to not only be a useful tool for the commission, but also for members of the public who are viewing and taking an interest.

Representative Day entertains a motion to make and post recordings, starting with today's meeting and going forward.

Commissioner Dave Rogers makes the motion to record our proceedings.

The motion is seconded.

Patrick Prendergast, staff member in the office of Representative Day, calls the roll in an expedited fashion.

The roll is called and unanimously approves to record proceedings.

The motion carries.

Representative Day notes that in pursuit of our charge the commission is going to request documentation, presentations, and a variety of sources to be discussed moving forward. The materials will be posted public. In advance of today's kick off, Representative Day notes he has directed his staff to create a website that's going to serve as the main repository for our meeting recordings, agendas, minutes. Representative Day asks Jacqui Manning, staff member in the office of Representative Day, to share her screen to show commission members the website.

Jacqui Manning displays the website for the Special Commission on Facial Recognition.

Representative Day asks if there are any discussions or questions on the website. No questions were raised to Representative Day.

Representative Day notes the charge states that the first meeting of the Special Commission on Facial Recognition to occur by February 15, and notes that it is now mid April. Representative Day explains that the COVID challenges prevented the committee from meeting the initial deadline but is very confident of meeting the reporting deadline of December 31, 2021.

Representative Day requests that commission members reserve the third Friday of every month as a placeholder for future meetings, and that all meetings date decisions will be made as a group. Representative Day asks if there are any comments or questions. No questions were raised to Representative Day.

Representative Day motions to move to agenda item three and asks Senator Eldridge to read the charge of the Special Commission on Facial Recognition.

Senator Eldridge reads the charge, Section 105 of Chapter 253 of the Acts of 2020, while the legislative staff shares the charge on the screen.

Representative Day notes the importance of reviewing the charge to ensure that we are meeting the tasks requested. Representative Day notes that the Chairs and legislative staff have lumped the charge into four broad topics out of those 12 specific charges that we thought would be helpful as a commission to have a discussion. Representative Day asks Jacqui Manning to share that outline on the screen.

The four broad topics outlined, along with the subcategories, are introduced by Representative Day.

Representative Day opens the meeting up for discussion in relation to the broad outline of the commission's charges to see if there are perspectives or thoughts on how we should move forward.

Representative Day recognizes Commissioner Kade Crockford.

Kade Crockford wonders if, given the commissions charge towards the end of the language to also consider the use of facial recognition to track people in public spaces, it might be useful to add something to this conversation about that use of the technology which is distinct from using the technology to perform image matching to identify someone in a still image.

Representative Day recognizes Commissioner Alicia Rebello-Paradas.

Commissioner Rebello-Paradas thanks Rep. Day and the legislative staff for their organization and work and seconds Commissioner Crockford's recommendation. Commissioner Rebello-Paradas wonders if one

starting point should be getting the RMV or the state police to produce an FR search at the next meeting so everyone is starting from the same point and is able to see how research is conducted.

Representative Day recognizes Commissioner Farnsworth.

Commissioner Farnsworth echoes Commissioner Rebello-Paradas' suggestion. Commissioner Farnsworth notes, after being involved in law enforcement for many years, he believes there is a large gap between how Facial Recognition is used on TV shows and how it's actually used and employed in MA. Commissioner Farnsworth believes it may be appropriate to understand how it is used, and more importantly, how it is not used in Massachusetts.

This notion is seconded.

Representative Day notes that the chairs wanted to start from a common base of understanding, and the idea behind organizing the charge into buckets was to start with the history and find out what's been utilized here in Massachusetts. Representative Day believes that if the commission can come to a base knowledge of what Facial Recognition is, how it's used, what it looks like, and really get a fundamental grasp on that I think that would be particularly useful. Representative Day asks Commissioner Colleen Ogilvie, Registrar of Motor Vehicles, is this something that the Commission can task her with registrability of coming up with a presentation.

Commissioner Ogilvie agrees to put together a presentation for the next meeting.

Representative Day expresses interest in the Commissioners who are in this field as scholars to come forward to tell us what would be most useful as we start digging in here going forward, here especially as the Commission is looking at the history and what the technology is and what it isn't. Representative Day recognizes Commissioner Learned Miller.

Commissioner Learned Miller notes that he has given quite a few tutorial talks on the basics of the technology and states that when people think it's the right time for something like that he would be happy to present.

Representative Day notes that the members are coming into this in different levels of expertise- some with very limited exposure to facial recognition and others obviously have devoted much of their professional lives to it. Representative Day airs on the side of over inclusion on what the commission is doing here so that everyone is able to get a base understanding. States that if the rest of the Commission agrees, that the Commission has a presentation from the RMV and a Dr. Lerner Miller at the next meeting to kind of get that fundamental base.

The notion is seconded.

Representative Day recognizes Commissioner John Woodward.

Commissioner Woodward proposes various organizations within the US government, such as the National Institute of Standards and Technology, which has done a great deal of work on facial recognition and I believes that some of their subject matter experts would be very useful to hear from. Commissioner Woodward notes names of potential presenters such as Jonathan Phillips or Patrick Grother of National Institute of Standards and Technology (NIST), Anil Jain at Michigan State University, and Dr. Michael King at Florida Institute of Technology and believes it would be beneficial for the Commission to really understand technical aspects of the technology because it will help us inform recommendations for policy making.

Representative Day recognizes Commissioner Dyson

Commissioner Dyson states that there are some concerns to be raised with regard to overview of face recognition technology software (outline item number 2) and potentially as it relates to outline item four with regard to the comparison of different facial recognition technologies. Commissioner Dyson believes it would be useful to also think about to what extent this state is actually working with third party vendors, data brokers, and other companies to basically contract out their services for use of this technology in those cases and that it would be helpful to be able to know who those might be and of course to see what auditing trails may be in existence for those technologies as well so that might be understood. Notes it should be on the record if it is not that for comparison of different local technologies that we should think about also the company we may be contracting out with to use those technologies that those are not owned by the Commonwealth

Representative Day recognizes Commissioner Hartzog

Commissioner Hartzog notes that one thing perhaps that was implicit within some of the concerns that are listed in Section 3 around privacy rights and due process rights but I do hope that we will be able to also discuss what might be considered downstream effects with facial recognition the way in which facial recognition and power is decision making systems and the way in which it is likely to be diploid and employment settings or to 2nd commissioner Crockfords proposal about thinking about privacy in public spaces as well that may not traditionally fall in what we think of as privacy rights to due process rights but certainly use personal information that have potential implications on our rights and protections so I just wanted to see if we could make that make sure that that was explicit as part of category three.

Representative Day recognizes Commissioner Brooks

Commissioner Brooks suggests also hearing from the Fusion center.

Representative Day notions Commissioner Brooks or Commissioner Range to explain what the Fusion Center is.

Commissioner Range acknowledges notion and explains the history of the Fusion Center.

- "Fusion center in Massachusetts was set up in 2004 after 911 and it was primarily focused on preventing acts of terrorism. Fusion Center in Massachusetts is one of the 80 recognized Fusion Centers across the country. Focused on all crimes & threats meaning it's not just specific to terrorism and the primary reason why is because a lot of it is based on behavior. Primary mission is focused on prevention and preventing acts or threats of violence and things like that from actually occurring. Fusion Center does use facial recognition- system is the RMV system. We've put some parameters in place to try and to ensure and we use it we're doing in a very thoughtful way is there"

Representative Day suggests that the RMV and State Police combine presentations for next meeting. Representative Day notes that it is sounding to me on this beginning piece that we've got two kind of threads here: 1. The real practice in Massachusetts which obviously is an element of charge- what the RMV does, how it utilized, what it is, and how the state police has been interacting with it. 2. Industry perspective that I think Commissioner Dyson was talking Representative Day notes that these are two kinds of united but distinct threads that we should be delving into here and wonders if the presentations can be fit into one meeting or should the presentations be broken up into two meetings.

Representative Day recognizes Commissioner Ogilvie.

Commissioner Ogilvie notes that depending on the amount of detail, the presentations could be completed in one meeting, and if more detail is needed we could continue in the future meeting.

Representative Day recognizes Commissioner Learned Miller

Commissioner Learned Miller states that there are two distinct goals: A working example which was one of the first things suggested. Commissioner Learned Miller believes it is a great idea there's nothing like having an example of how it's really used as structure for conversations. Notes that at the same time, clearly the Commission wants to consider all the ways it's used in the state and that's something that can be done over a longer period of time. Commissioner Learned Miller does not think it has to be done in the first meeting.

Representative Day recognizes Commissioner Brooks

Commissioner Brooks seconds the notion that the presentations can be completed in one meeting

Representative Day recognizes Commissioner Rogers

Commissioner Rogers notes one point he is interested in exploring is part of the third category on due processes and how facial recognition technology is playing out in criminal procedure and that it might be helpful to the Commission to understand how law enforcement use of this technology how it manifest in the courtroom and the rights of those accused.

Representative Day recognizes Commissioner Creem

Commissioner Creem notes concern about facial recognition issues raised in other forms of biometric rather than just facial recognition

Representative Day notes that there are many areas in the FR charge where we can go off track due to the expansive area of the topic, and notes that we will have to limit the scope of where our charge goes but does agree with Commissioner Creem that we are limited in respect to our report, but that does not mean we cannot go outside the scope of our charge to be informed about facial recognition technology in other ways.

Representative Day recognizes Commissioner Alicia Rebello Paradas

Commissioner Rebello Paradas notes back to Commissioner Rogers' comment about bucket three in relation to the different roles for law enforcement in the you know traditional state police, local, municipal police departments and then there might be a different role in facial recognition for the prosecutors office so I think it's just something to keep in mind that as you know we have this these buckets there's going to be even further smaller buckets and that just may be too much too far into the weeds and and something we just make note about in the report but everyone has a different role when it comes to the use of this technology and even how it's stored but that just might be beyond our charge but it's something just to keep in mind.

Representative Day recognizes Commissioner O'Keefe

Commissioner O'Keefe emphasizes the rights of the individual citizen but also the importance of using FR to enhance public safety. Seems there is a task of understand that the technology is a good thing but notes the concerns around its accuracy. Commissioner O'Keefe suggests the formation of subcommittees to break down the different charges.

Representative Day recognizes Commissioner Crockford

Commissioner Crockford wants to second Commissioner Rogers comment about the importance of looking at how facial recognition information makes its way into criminal cases, how information is shared with prosecutors and how prosecutors share that information with defendants. Commissioner Crockford think that's a really key question and given that looking at some of the due process issues is a charge of this. I just wanted to quickly address something that commissioner will keep just said you know in the civil rights and civil liberties community we are obviously very concerned about the tendency that many of these technologies have to be racially biased to work less well for frankly everyone except for middle aged white men unfortunately but that's not nearly the the full range of our concerns we also have significant concerns about the use of the technology to identify people in a variety of contexts where you know we think it would be inappropriate so just wanted to state for the record that that our concerns are not merely about accuracy or reliability they're also about you know frankly the power of a technology that essentially enables governments to identify someone who's just walking down the street minding their own business and is you know could be used in a way that could essentially you know translated to everyone walking around with their personal information tattooed on their face so just wanted to express that there may be a difference in in viewpoints on that particular.

Representative Day recognizes Commissioner Spurlock

Commissioner Spurlock seconds Commissioner Crockfords statement and does not think, at least from the criminal defense perspective, that the only or even the main problem with this technology is its accuracy that we also have serious concerns with the invasiveness of this technology. Believes it would be wrong to assume that we're all on the same page about that being the main problem here although it certainly is one that we should address as well.

Representative Day recognizes Commissioner Rogers

Commissioner Rogers respectfully pushes back at the notion that it's generally agreed that this technology is a good thing but there are concerns about reliability the reliability is 1 bucket but clearly the 4th amendment our freedom as American citizens to be free from unreasonable search and seizure the inherent rights to privacy and this technology has gotten ahead of the law the version of the bill that passed the law that is now law in the house as I'm sure people know how to warrant requirement and in the end a compromise was reached and so we're glad to have a new law on the books that put some constraints on the technology but it certainly does bring up significant concerns about if someone's been identified in this way they have a right to know that they were right to challenge it in so I think we I think as part of the due process and within the charge of the Commission

Representative Day notes that there are no more questions or comments from Commissioners but notes that we should think about Commissioner O'Keefe's comments on the subcommittee to be discussed at the next meeting.

Senator Eldridge concurs that we revisit the creation of subcommittees at the next meeting

Representative Day recognizes Commissioner Ogilvie

Commission Ogilvie notes to establish subcommittees for the topics that will take the most time and research so those can be formed quickly

Representative Day motions to task everyone on the commission to do homework on what they believe would be the appropriate subcommittee or subcommittees and start to have that discussion prior to the next meeting so we hit the ground running. Representative Day also requests to give thought to particular presentations and reminds that the commission needs to be done well in advance of the report deadline so the report can be drafted and have the options for edits or comments. Representative Day asks members if there are any further comments or concerns on the next steps.

Commissioner Ogilvie wants to confirm the time for her presentation next week out of the hour and a half.

Commissioner Rebello Paradas flags that open meeting laws will also apply to subcommittees.

Representative Day notes that a discussion on this should be and the different interpretation on the requirements there

Commissioner Crockford notes an interest in making sure all other commissioners have a window into what's going on if we decide to go down the road of subcommittees in each subcommittee and the opportunity to participate.

Representative Day notes that the intent is to split up the work more than anything and then report back in a regular fashion and information would certainly be available as that work product is generated. Representative Day then recognizes the next steps for the commission is to ask Major Range and Registrar Ogilvie to pull together a presentation for us on the use and background of the technology in play here in Massachusetts right now and asks everyone to start thinking through what kind of data we need, what sources we want, and ask some of our professors here for recommendations on further presentations on the industry side of things.

Commissioner Woodward asks what is the best way to communicate these ideas?

Representative Day defers to legislative staff, who provide their email information in the chat on Microsoft Teams.

Representative Day recognizes Professor Learned Miller

Professor Learned Miller requests to confirm that he is presenting at the next meeting

The consensus is agreed that the next meeting, which is set for Friday, May 21 at 11 AM, will start with a presentation from the State Police/ RMV followed by a 30-minute presentation from Professor Learned-Miller.

Representative Day entertains a motion to adjourn with our next meeting being Friday, May 21 at 11:00 AM.

The motion is seconded and the meeting is adjourned.

Special Commission on Facial Recognition Meeting Minutes
Friday, May 21, 2021 at 11:00 a.m.
(Virtual Meeting)

Agenda

- I. Introduction/Roll Call
- II. Approval of Minutes from 4.16.21 Meeting
- III. Presentation from Professor Erik Learned-Miller
- IV. Presentation from Registry of Motor Vehicles and State Police
- V. Review and Discussion of Statutory Charge
- VI. Discussion of Potential Subcommittees
- VII. Discussion of Topics for Future Meetings
- VIII. Schedule Next Meeting

Chair Eldridge called the meeting to order and indicated that Chair Day would be unable to join. Rep. Rogers served as the House Co-Chair for this meeting of the Commission.

Chair Eldridge noted that the Chairs received a letter from Chief Justice Kimberly Budd, informing them that neither she nor any appointee of hers would be participating in the work of the Commission. A copy of that letter would be posted on the Commission website.

Chair Eldridge directed that a roll call of the Commission be taken.

Commissioners Present:

Chair Eldridge
Commissioner Rogers
Commissioner Woodward
Commissioner Hartzog
Commissioner Dyson
Commissioner Gomez
Commissioner Creem
Commissioner Brooks
Commissioner Cordy
Commissioner Rebello-Pradas
Commissioner Farnsworth
Commissioner Ogilvie
Commissioner Learned-Miller
Commissioner Range
Commissioner Crockford
Commissioner Spurlock
Commissioner Nkonde
Commissioner Verma
Commissioner O’Keefe
Commissioner Conley

Commissioners Absent:

Chair Day

Chair Eldridge asked the Commissioners to review the minutes from the Commission meeting on April 16, 2021 Commission meeting and offer any edits or comments. Edits and comments were given by several Commissioners and noted for the record.

Chair Eldridge asked for a motion to approve the minutes as edited. There was a motion made by Commissioner Rebello-Pradas, seconded by Commissioner Creem, and the motion passed unanimously.

Chair Eldridge noted the importance of reviewing the statutes and regulations for all states regarding facial recognition, including cities in Massachusetts.

Chair Eldridge asked if anyone was aware of any compilation of what the 50 states have done around facial recognition. Commissioners Rebello-Pradas and Creem suggested checking with NCSL.

Chair Eldridge asked if any commission members would like to work on the issue and proposed creating a working group to gather data and information for the full commission. Commissioners Crockford, Nkonde, O'Keefe, Woodward, Rebello-Pradas, and Dyson volunteered.

Commissioner Professor Learned-Miller gave a presentation on "Facial Recognition Technology" and then fielded questions from members.

Commissioner Acting Registrar Colleen Ogilvie then presented on "RMV's Utilization of Facial Recognition Software to Detect and Prevent Fraud" and fielded questions from members.

Commissioner Major Scott Range then presented on the State Police's use of facial recognition technology and fielded questions from members.

The statutory charge was then read for review by the Commission.

Chair Eldridge asked members to email Judiciary Committee staff suggestions for possible subcommittees.

Chair Eldridge announced the next Commission meeting, thanked Commissioners for their work and participation, and ended the meeting.

Special Commission on Facial Recognition Meeting Minutes
Friday, July 9, 2021 at 1:00 p.m.
(Virtual Meeting)

Agenda:

- I. Introduction/Roll Call
- II. Approval of Minutes from 5.21.21 Meeting
- III. Discussion of Facial Recognition Limitation in Police Reform
- IV. Discussion of Facial Recognition Limitations in Other Jurisdictions
- V. Review of Statutory Charge
- VI. Discussion of Topics for Future Meetings
 - a. Public Input
 - b. Information Requests to Local Law Enforcement and Prosecutors
- VII. Schedule Next Meeting

Chair Day opened the meeting, welcomed members, and made introductory remarks.

Chair Day recognized Chair Eldridge who made introductory remarks.

Chair Day directed that a roll call of the Commission be taken.

Commissioners Present:

Chair Day
Chair Eldridge
Commissioner Rogers
Commissioner Woodward
Commissioner Hartzog
Commissioner Dyson
Commissioner Cordy
Commissioner Rebello-Pradas
Commissioner Ogilvie
Commissioner Learned-Miller
Commissioner Range
Commissioner Crockford
Commissioner Spurlock
Commissioner Nkonde
Commissioner Verma
Commissioner Conley

Commissioners Absent:

Commissioner Gomez (Lauren Matteodo appeared on his behalf)
Commissioner Creem
Commissioner Brooks
Commissioner Farnsworth
Commissioner O'Keefe

Chair Eldridge asked Commissioners to review minutes from the May 21, 2021 Commission meeting and offer any edits or comments. No comments or edits were made. Chair Eldridge asked for a motion to approve the minutes. There was a motion made by Commissioner Rebello-Pradas, seconded by Commissioner Hartzog, and the motion passed unanimously.

Commissioner Crockford provided a presentation on facial recognition legislation in other jurisdictions and then fielded questions from members.

Chair Day provided a presentation on facial recognition legislation included in Chapter 253 of the Acts of 2020 (Police Reform Law) and then fielded questions from members.

The commission reviewed the statutory charge.

Chair Day then opened the commission up to a discussion on potential topics for future meetings. Chair Day suggested inviting public input at the next meeting to take place at the end of July. He then suggested requesting information from local law enforcement about their past and current use of facial recognition for discussion at the following meeting to take place in September.

Commissioners supported the Chair's suggestions and further discussed what information to request and which agencies to request information from. Commissioner Crockford suggested creating a survey for law enforcement agencies to fill out, so there is uniformity in information requested and received. Commissioner Rebello-Pradas requested that Commissioners be able to review the requests before they go out. Chair Day agreed and suggested that Commissioners email Judiciary Committee General Counsel Dianna Williams with any questions or information that they would like included.

Chair Day noted that, after these next two meetings, the Commission will be in a better position to engage in more substantive policy discussions.

Chair Day noted that the next meeting would take place on Friday, July 30, 2021, likely at 11 a.m., thanked Commissioners for their work, made closing remarks, and requested a motion to adjourn.

Chair Eldridge made closing remarks and moved to end the meeting. Commissioner Crockford seconded and the meeting ended.

Special Commission on Facial Recognition Meeting Minutes
Friday, July 30, 2021, at 11:00 A.M.
(Virtual Meeting)

Commissioners Present:

- Chair Eldridge
- Chair Day
- Commissioner Rogers
- Commissioner Woodward
- Commissioner Hartzog
- Commissioner Gomez
- Commissioner Creem
- Commissioner Cordy
- Commissioner Farnsworth
- Commissioner Ogilvie
- Commissioner Range
- Commissioner Crockford
- Commissioner Spurlock
- Commissioner Nkonde
- Commissioner Verma
- Commissioner Conley
- Commissioner O’Keefe
- Commissioner Rebello-Pradas
- Commissioner Learned-Miller
- Commissioner Dyson

Commissioners Absent:

- Commissioner Brooks

Chair Eldridge called the meeting to order, and he and Chair Day gave introductory remarks. Chair Eldridge invited a motion to approve minutes circulated for the July 9, 2021, meeting. Motion made by Commissioner Crockford, seconded by Chair Day, and unanimously approved by members present.

Chair Eldridge began the public testimony portion of the meeting. Commissioners heard from various persons and organizations regarding government use of facial recognition technology in the Commonwealth.

Chair Day led a review of draft information requests to local law enforcement and prosecuting agencies and solicited feedback from Commissioners on the content and format of the requests.

Chair Day led a discussion on topics for future commission meetings, including inviting specific facial recognition users and companies to speak to the commission.

Chair Eldridge noted that the next meeting would take place after Labor Day, made closing remarks, and ended the meeting.

Special Commission on Facial Recognition Meeting Minutes
Friday, September 17, 2021, at 11:00 A.M.
(Virtual Meeting)

Agenda:

- I. Introduction/Roll Call
- II. Approval of Minutes from 7.30.21 Meeting
- III. Review of Responses to Initial Survey
- IV. Discussion of Follow Up Survey
- V. Discussion of Topics for Future Meetings
- VI. Schedule Next Meeting

Commissioners Present:

- Chair Day
- Chair Eldridge
- Commissioner Rogers
- Commissioner Creem
- Commissioner Brooks
- Commissioner Cordy
- Commissioner Ogilvie
- Commissioner Range
- Commissioner Crockford
- Commissioner Spurlock
- Commissioner Verma
- Commissioner O’Keefe
- Commissioner Rebello-Pradas
- Commissioner Learned-Miller
- Commissioner Dyson
- Commissioner Conley
- Commissioner Woodward

Commissioners Absent:

- Commissioner Hartzog
- Commissioner Gomez
- Commissioner Farnsworth
- Commissioner Nkonde

Chair Day called the meeting to order and gave introductory remarks.

Chair Day invited a motion to approve minutes circulated for the July 30, 2021, meeting. No comments or edits were made. Motion made by Chair Eldridge, seconded by Commissioner Ogilvie, and unanimously approved by members present.

Chair Day recognized Major Scott Range on his retirement and congratulated him on behalf of the commission.

The Commission reviewed and discussed responses received thus far to the Initial Survey sent to law enforcement and prosecuting agencies.

The Commission reviewed and discussed questions to be included in a Follow-Up Survey to law enforcement and prosecuting agencies who responded affirmatively to using facial recognition technology in the Initial Survey.

Chair Day noted that the next meeting is scheduled to take place on October 15, 2021, at 11 am, and will include a review of responses to the Follow-Up Survey, discussion of topics for future meetings, and plan for commission deliberations.

Chair Day gave closing remarks and welcomed a motion to adjourn the meeting. Chair Eldridge moved, Commissioner O'Keefe seconded, and the meeting ended.

Special Commission on Facial Recognition Meeting Minutes
Friday, October 15, 2021, at 11:00 A.M.
(Virtual Meeting)

Agenda:

- I. Introduction/Roll Call
- II. Approval of Minutes from 9.17.21 Meeting
- III. Status Update on Initial and Follow-Up Surveys
- IV. Review of Statutory Charge
- V. Open Discussion Amongst Commissioners
- VI. Discussion of Topics for Future Meetings
- VII. Schedule Next Meeting

Commissioners Present:

- Chair Day
- Chair Eldridge
- Commissioner Rogers
- Commissioner Woodward
- Commissioner Creem
- Commissioner Brooks
- Commissioner Rebello-Pradas
- Commissioner Farnsworth
- Commissioner Ogilvie
- Commissioner Learned-Miller
- Commissioner Cyr
- Commissioner Crockford
- Commissioner Spurlock
- Commissioner Verma
- Commissioner O’Keefe
- Commissioner Dyson
- Commissioner Gomez

Commissioners Absent:

- Commissioner Cordy
- Commissioner Hartzog
- Commissioner Nkonde
- Commissioner Conley

Chair Eldridge called the meeting to order, gave introductory remarks, and welcomed Major Mark Cyr, who is replacing Major Scott Range on the Commission.

The Commission reviewed the minutes circulated for the September 17, 2021, meeting. No comments or edits were made. Motion made by Chair Day, seconded by Commissioner O’Keefe, and unanimously approved by members present.

Chair Eldridge gave an update on responses to the initial and follow up surveys sent to law enforcement and prosecuting agencies regarding their use of facial recognition.
The Commission read and reviewed the statutory charge.

The Commission then engaged in an open discussion regarding government use of facial recognition in the Commonwealth, including the use of facial recognition before Chapter 253 of the Acts of 2020

(commonly referred to as “Police Reform Law”), facial recognition after Police Reform Law, the regulation of facial recognition in other jurisdictions, observations and concerns relative to the use of this technology, and recommendations for future use.

Chair Eldridge advised that the next meeting is scheduled to take place on Friday, November 19, 2021, at 11:00 am.

Chair Eldridge and Chair Day gave closing remarks and the meeting ended.

Special Commission on Facial Recognition Meeting Minutes
Friday, November 19, 2021, at 11:00 A.M.
(Virtual Meeting)

Agenda:

- VIII. Introduction/Roll Call
- IX. Approval of Minutes from 10.15.21 Meeting
- X. Status and Disclosure of Survey Responses
- XI. Review of Report Outline
- XII. Continued Open Discussion
- XIII. Schedule Next Meeting

Commissioners Present:

- Chair Day
- Chair Eldridge
- Commissioner Woodward
- Commissioner Dyson
- Commissioner Creem
- Commissioner Brooks
- Commissioner Rebello-Pradas
- Commissioner Farnsworth
- Commissioner Ogilvie
- Commissioner Learned-Miller
- Commissioner Cyr
- Commissioner Crockford
- Commissioner Spurlock
- Commissioner O’Keefe
- Commissioner Conley
- Commissioner Hartzog
- Commissioner Nkonde
- Commissioner Verma

Commissioners Absent:

- Commissioner Rogers
- Commissioner Gomez – Danielle Howard representing
- Commissioner Cordy

Chair Day called the meeting to order and gave introductory remarks.

The Commission reviewed the minutes circulated for the October 15, 2021, meeting. No comments or edits were made. Motion to approve made by Chair Eldridge, seconded by Commissioner O’Keefe, and unanimously approved by members present.

Chair Day gave an update on responses received to the surveys sent to law enforcement and prosecuting agencies regarding their use of facial recognition.

The Commission read and reviewed the report outline and statutory charge.

The Commission then engaged in an open discussion regarding government use of facial recognition in the Commonwealth, including government use of facial recognition beyond law enforcement, observations and concerns relative to the use of this technology, and recommendations for future use.

Chair Eldridge advised members that the next meeting is scheduled to take place on Friday, December 17, 2021, at 11:00 am.

Chair Day and Chair Eldridge gave closing remarks. Motion to adjourn was made by Chair Eldridge and seconded by Commissioner O'Keefe. The meeting ended.

Special Commission on Facial Recognition Meeting Minutes
Friday, December 17, 2021, at 11:00 A.M.
(Virtual Meeting)

Agenda:

- XIV. Introduction/Roll Call
- XV. Approval of Minutes from 11.19.21 Meeting
- XVI. Review of Statutory Charge
- XVII. Survey Response Update
- XVIII. Discussion of Possible Report Recommendations
- XIX. Discussion of Draft Report
- XX. Schedule Next Meeting

Commissioners Present:

- Chair Day
- Chair Eldridge
- Commissioner Rogers
- Commissioner Woodward
- Commissioner Hartzog
- Commissioner Dyson
- Commissioner Gomez – Danielle Allard representing
- Commissioner Creem
- Commissioner Brooks
- Commissioner Cordy
- Commissioner Farnsworth
- Commissioner Ogilvie
- Commissioner Cyr
- Commissioner Crockford
- Commissioner Spurlock
- Commissioner Nkonde
- Commissioner Conley
- Commissioner Rebello-Pradas

Commissioners Absent:

- Commissioner Learned-Miller
- Commissioner Verma
- Commissioner O’Keefe

Chair Eldridge called the meeting to order, gave introductory remarks.

The Commission reviewed the minutes circulated for the November 19, 2021, meeting. No comments or edits were made. Motion made by Commissioner Ogilvie, seconded by Chair Day, and unanimously approved by members present.

The Commission began with a review of the statutory charge.

The Commission moved to a review of initial and follow-up survey responses.

The Commission then engaged in a presentation and discussion of possible report recommendations regarding government use of facial recognition in the Commonwealth which largely focused on

observations and concerns relating to law enforcement use. Commissioner Woodward gave a presentation on his thoughts and recommendations for regulation and discussion amongst the commission continued.

Chair Eldridge noted that no further meetings are currently scheduled, but that could be subject to change.

Chair Day and Chair Eldridge thanked the committee and gave closing remarks. The meeting ended.

Appendix D
Initial Survey Template

Massachusetts Special Commission on Facial Recognition
INITIAL SURVEY TO LAW ENFORCEMENT AND PROSECUTING AGENCIES
<https://frcommissionma.com/>

The Massachusetts Special Commission on Facial Recognition, which was established under [Section 105 of Chapter 253 of the Acts of 2020](#), respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or department's use or review of facial recognition (FR) technology or FR search results **within the last three (3) years**. We ask that you please respond to this initial survey by **September 6, 2021**.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

1. Has your office or department ever used facial recognition technology, directly or indirectly?

A. Yes. We currently use FR.

A1: If yes, how long you have used it?

A2: How many facial recognition searches have you run?

[0-5]

[6-10]

[11-20]

[21-50]

[Over 51]

B. Yes. We used or tested FR, but no longer use or test it.

C. We do not currently use FR, but we have plans to use it.

D. We do not currently use FR and have no plans to use it.

2. Has your office or department ever entered into a contract or other relationship with a company for the lease, use, possession, or other provision of facial recognition technology?

A. Yes.

B. No.

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a temporary basis?

A. Yes.

B. No.

4. Has anyone from your office or department ever requested that an out-of-state, federal, state, or local agency, including, but not limited to, the Massachusetts State Police, Registry of Motor Vehicles, or FBI, or a non-governmental organization perform a facial recognition search for your office or department or anyone in it?

A. Yes.

B. No.

5. **Has anyone from your office or department ever been involved in an interagency investigation during which any federal, state, or local government agency or non-government organization used facial recognition technology?**
 - A. Yes.
 - B. No.
6. **Has your office or department ever prosecuted a case resulting from a criminal investigation during which facial recognition technology was used?**
 - A. Yes.
 - B. No.
7. **If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:**

Appendix E

Summary of Initial Survey Responses

Organization	1A. Has your office or department ever used facial recognition technology, directly or indirectly? (Direct use might involve someone from your office using facial recognition software supplied by a vendor. Indirect use might involve someone from your office)	1B. If you answered YES to 1A, how long you have used FR technology? If you answered NO to 1A, please skip this question.	1C. If you answered YES to 1A, how many facial recognition searches have you run or reviewed? If you answered NO to 1A, please skip this question.	2. Has your office or department ever entered into a contract or other relationship with a company for the lease, use, possession, or other provision of facial recognition technology?	3. Has your office or department, or any agent or employee of your office or department, ever tested facial recognition technology?	4. Has anyone from your office or department ever requested that another agency (local, state, federal, or out of state), including, but not limited to, the Massachusetts State Police, Registry of Motor Vehicles, or FBI, or a non governmental organization	5. Has anyone from your office or department ever been involved in an interagency investigation during which any federal, state, or local government agency or non government organization used facial recognition technology?	6. Has your office or department ever prosecuted a case resulting from a criminal investigation during which facial recognition technology was used?	7. If there is any additional information that you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:
Acton Police Department	Yes. We used or tested FR, but no longer use or test it.	Several years ago/external agency	0-5	No	No	Yes	No	No	Our department utilized FR to identify a pedestrian who was struck by a motor vehicle with serious injuries. We were able to positively identify the pedestrian and notify the family.
Acushnet Police Department	Yes. We used or tested FR, but no longer use or test it.	1 time in about 2017-2018	0-5	No	No	Yes	No	No	The one time we attempted to utilize facial recognition was about 4 years ago. We used the now defunct option in the CopLink mobile app in an attempt to confirm someone's identity while live on the scene of an investigation.
Amherst	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Amherst College Police	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Animal Rescue League of Boston Law Enforcement Department	We do not currently use FR and have no plans to use it.			No	No	Yes	No	No	
Aquinnah Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Arlington Police Department	Yes. We used or tested FR, but no longer use or test it.	We have used it in the past a few times	0-5	No	No	Yes	Yes	No	It's a valuable investigative tool
Ashby Police	Yes. We used or tested FR, but no longer use or test it.			No	No	Yes	Yes	No	
Ashfield Police	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Auburn PD	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Ayer Police Department	We do not currently use FR and have no plans to use it.			No	No	Yes	No	No	
Bedford Police	We do not currently use FR, but we have plans to use it.			No	No	Yes	Yes	No	
Belchertown Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Bellingham Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	No
Berkshire District Attorney's Office				No	No	No		No	Re: Question 1 My office has never used FRT and we don't have plans to use it except when and if upon review of the technology we find it to be productive and helpful in responding to an emergency situation (ie. I like the Boston Marathon Bomber situation) or in solving a serious, violent crime. We would not rely solely on the technology in making an arrest but may use it as a lead in an emergency situation or solving a serious, violent crime. Re: Question 5 FTR has not been used in a Berkshire County investigation to my knowledge but I can't speak for the Federal government.
Berlin Police Department	We do not currently use FR and have no plans to use it.			No	No		No	No	
Barnstable Police Department	We do not currently use FR and have no plans to use it.								
Beverly Police	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Blackstone Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Boston	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Bourne Police	We do not currently use FR, but we have plans to use it.			No	No	No	No	No	
Boxborough Police Department	We do not currently use FR and have no plans to use it.			No	Yes	No	No	No	It would seem reasonable to have this technology available to build leads on cases.
Boylston PD	We do not currently use FR and have no plans to use it.			No	No	No	No	No	No
BrainTree Police Department	We do not currently use FR and have no plans to use it.			No	No	Yes	Yes	Yes	
Brewster, MA Police Department	We do not currently use FR and have no plans to use it.			Yes	Yes	No	No	No	
Bristol Community College	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Bristol County DA Office				No	No	No		No	With respect to Question 1, my answer would be we will use it when and if upon a review of the technology we find it to be productive and helpful in solving a serious crime. With respect to Question 5, my answer would be in joint Federal/State investigations we do not always know what the Feds are doing.
Brookfield Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Brookline Police Dept.	We do not currently use FR and have no plans to use it.			No	No	Yes	Yes	No	Town of Brookline has banned use of FR
Burlington Police Department	We do not currently use FR and have no plans to use it.			No	Yes	Yes	Yes	No	These answers are to the best of my knowledge. I have lost four senior detectives to retirement over the last year and the "Yes" answers to the above were based on their collective experiences - not attributable to the replacement personnel.
Carver Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Chelmsford Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Chelsea Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	

Cheshire Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	None	
Chester-Blandford Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No		
Clinton Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No		
Cohasset Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Danvers Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No		
Dartmouth Police Department	We do not currently use FR and have no plans to use it.	No	No		No	No	With the dramatic increase of video evidence available, I can see where reliable facial recognition technology may be able to assist with suspect identification. We have been very successful with identification by posting photos of subjects on social media and having the public identify them.	
Dedham Police Department	Yes. We used or tested FR, but no longer use or test it.	Indirectly through the state police several times over the years	0-5	No	No	Yes	Yes	No
Deerfield Police	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Dover Police Department	We do not currently use FR, but we have plans to use it.	No	No	No	No	Yes	No	
Dudley Massachusetts	Yes. We used or tested FR, but no longer use or test it.	We tested for app 6 months but program never officially began	0-5	No	Yes	No	No	No
								This is an excellent tool for investigation purposes to provide a list of potential suspects. It is never used as a sole or stand alone reason for a criminal charge. This technology exists. Data is used from public or otherwise available databases and is not intrusive. People voluntarily use facial recognition to open their phones. There is no reason why this cannot be used to help solve crimes. Again, it is only one part of the probable cause for investigation purposes. The fact the false narrative that people are being arrested and charged solely because of this technology, is completely ridiculous. This should be used by and available to law enforcement. If it can solve a murder, sexual assault of a child, or other violent crimes, it is worth it. Thank you for your time and consideration.
East Brookfield Police Dept.	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
East Longmeadow Police Department	We do not currently use FR and have no plans to use it.	No	No	Yes	Yes	No	No	
Easthampton MA PD	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Easton Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Edgartown PD	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	N/A
Essex DA	We do not currently use FR, but we have plans to use it.	No	No	No	Yes	Yes	Yes	* This office would use it if and when useful and productive in solving a serious crime and/or assisting in excluding suspects.
Essex Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Fairhaven Police Dept.	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Falmouth Police Department	We do not currently use FR and have no plans to use it.	No	No	No	Yes	No	No	
Foxborough Police Department	We do not currently use FR and have no plans to use it.	No	Yes	No	No	No	No	There are several companies offering free trials on this stuff in Massachusetts
Franklin MA PD	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Freetown Police Department	We do not currently use FR and have no plans to use it.	No	No	Yes	No	No	No	
Georgetown Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Gil Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	no
Glooucester Police Department	We do not currently use FR, but we have plans to use it.	No	No	No	No	No	No	We have not used it but wouldn't rule out using it in the future through a 3rd party (Fusion Center)
Grafton Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	We would utilize FR during an investigation into a serious crime if it was available and crucial to the outcome.
Granby Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Groveland Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Gt Barrington Police	We do not currently use FR and have no plans to use it.		No	No	No	No	No	
Hadley Police	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Halifax Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Hamilton Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	N/A
Hampden Police	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Hanson Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Haverhill Police	We do not currently use FR and have no plans to use it.	No	No	Yes	Yes	Yes	Yes	
Hingham Police Department	We do not currently use FR, but we have plans to use it.	No	No	Yes	Yes	Yes	Yes	
Holbrook Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Holyoke Community College Campus Police	We do not currently use FR, but we have plans to use it.	No	No	No	No	No	No	
Hopedale Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Hudson MA Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Hull Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Huntington	We do not currently use FR and have no plans to use it.	No	No	No	No	No	No	
Ipswich Police Department	We do not currently use FR and have no plans to use it.	No	No	No	Yes	No	No	

Kingston Police Department	Yes. We currently use FR (please answer questions 1B and 1C).	Sporadically for 4 years	0-5	No	No	Yes	Yes	Yes	Minimal use through 3rd party information sharing partners to solve serious crime.
Lase I University Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Lawrence Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Lee Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	questions 4 and 5 are as far as I am aware, but not certain.
Leicester Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Lenox Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Leverett PD	We do not currently use FR and have no plans to use it.			No	No	No	No	No	none
Littleton Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Longmeadow Police Department	We do not currently use FR and have no plans to use it.	N/A		No	No	No	No	No	
Ludlow, Massachusetts, Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Lunenburg Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Lynn Police Department	We do not currently use FR, but we have plans to use it.			No	No	Yes	No	No	
Marborough Police Department	Yes. We used or tested FR, but no longer use or test it.	Requested through State police several years ago	0-5	No	No	Yes	Yes	No	
Massachusetts State Police	Yes. We currently use FR (please answer questions 1B and 1C).	Since 2006		Yes	Yes	Yes	Yes	Yes	
Mattapoisett Police	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Mannard PD	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Medway Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Melrose Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Milbury Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Milton Police Department	Yes. We currently use FR (please answer questions 1B and 1C).	Rare, Occasionally over few years	0-5	No	No	Yes	Yes	Yes	Rarely used, but valuable tool. Always corroborate information.
Monson PD	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Montague Police	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Mt. Wachusett Community College	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Nantucket Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	Some of these questions should have given us the option to check "unknown". Without checking with every officer I cannot be sure that some of these answers are correct.
Natick Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Needham Police	We do not currently use FR and have no plans to use it.			No	No	Yes	Yes	Yes	
Norfolk District Attorney's Office	We do not currently use FR and have no plans to use it.			No	No	No	No	Yes	
Northampton Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	Our City Council passed an ordinance that bans the use of facial recognition by City employees.
Northborough Police Department	We do not currently use FR and have no plans to use it.			No	No	Yes	No	No	
Northwestern District Attorney's Office	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Norwood Police Department	Yes. We currently use FR (please answer questions 1B and 1C).	Since 2006	51 or more	Yes	No	Yes	Yes	Yes	Facial Recognition uses a point/grade system to match faces. Officers utilize the point/grade system to determine/corroborate if the match is good or not. Facial Recognition is just another tool to assist in identifying unknown suspects. It helps build towards probable cause, but it is not probable cause itself. You need to corroborate the match and have other evidence to support the match as well. It is a necessary tool for law enforcement which has led to many identifications of suspects that would not have been identified otherwise. The Norwood Police Department and NORPAC Task Force rely upon the availability and results provided by facial recognition systems/technology.
Office of District Attorney Marian Ryan	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Office of the Cape & Islands District Attorney				No	No	No		No	With respect to Question 1, my answer would be we will use it when and if upon a review of the technology we find it to be productive and helpful in solving a serious crime. With respect to Question 5, my answer would be in joint Federal/State investigations we do not always know what the Feds are doing.
Orange Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Orleans Police	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Peabody	Yes. We used or tested FR, but no longer use or test it.	6-10		No	Yes	Yes	Yes	No	No
Pelham Police Dept	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
PETERSHAM POLICE DEPARTMENT	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Pittsfield PD	Yes. We currently use FR (please answer questions 1B and 1C).	2 years	0-5	No		Yes	Yes	No	We only utilize the services provided by the Fusion Center based on RMV License photos.
Plainville Police Department	We do not currently use FR and have no plans to use it.			No	Yes	Yes	Yes	Yes	The use of facial recognition is a valuable tool and can be used to develop leads for investigative purposes. The technology should be used as an investigative tool but should be utilized similar to other ways of identification i.e. fingerprinting etc. Understanding ones facial recognition is immediately accessible and identifiable to the general public. Hence the anonymity of and individuals fingerprints would be protected further than and individuals facial characteristics.
Plymouth County DA	We do not currently use FR and have no plans to use it.			No	No	No	No	No	These answers are to the best of my available information and belief at this time

Plymouth Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Princeton Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Quinsigamond Community College Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	n/a
RANDOLPH POLICE DEPT.	Yes. We used or tested FR, but no longer use or test it.	We have not used in several years	6-10	No	No	Yes	Yes
Revere Police Department	We do not currently use FR and have no plans to use it.	No	No	Yes	Yes	Yes	Only facial recognition has been through the RMV - nothing recently.
Rockport Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Rowley Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Salem Police Department	We do not currently use FR and have no plans to use it.	No	No	Yes	Yes	Yes	
Salisbury Police Dept.	We do not currently use FR and have no plans to use it.	No	No	No	No	No	none
Schubert Police Department	We do not currently use FR and have no plans to use it.	No	Yes	No	No	No	
Shirley Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Shrewsbury	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Somerset Police Department	Yes. We used or tested FR, but no longer use or test it.	It was used on one occasion by the detective division in an attempt to solve a bank robbery	0-5	No	Yes	No	No
South Hadley Police Department	We do not currently use FR, but we have plans to use it.				No	No	No
Southampton Police Department	We do not currently use FR, but we have plans to use it.	No	No	No	No	No	
Southwick	Yes. We currently use FR (please answer questions 1B and 1C).	Several years	11-20	No	No	Yes	Yes
Springfield technical Community College	We do not currently use FR and have no plans to use it.	No	No	No	No	No	FR can be a very helpful tool for law enforcement when attempting to identify suspects.
Stoneham Police Department	Yes. We used or tested FR, but no longer use or test it.	0-5	No	No	Yes	Yes	None.
Stoughton	We do not currently use FR and have no plans to use it.	No	No	Yes	Yes	No	Use of FRT was in one fraud case. Suspect was identified through a non-governmental agency. Case was referred to authorities in Georgia.
Sturbridge Police	We do not currently use FR and have no plans to use it.	No	No	No	No	No	The Stoughton Police Department has not used any facial recognition technology from any agency in more five years.
Sudbury Police Department	We do not currently use FR and have no plans to use it.	No	Yes	No	No	No	Only tested/investigated relative to body camera initiative.
Suffolk County DA	Yes. We currently use FR (please answer questions 1B and 1C).	Directly for 2 years; indirectly for 15+.	51 or more	Yes	Yes	Yes	Yes
While public safety and privacy interests seem to be often in conflict in this space, the true value of these tools and their contribution to public safety and public health seldom get adequate representation. There are several critical areas that facial recognition tools tip heavily to the public safety side of the spectrum that should be mentioned; they include counterterrorism and critical incident response, transportation security, and investigations into missing and exploited children. The last one, investigations into missing and exploited children, is the one we can speak to most adequately based on our Office's current work. The nonprofit group Thorn which provides a tool called Spotlight (which we use in conjunction with an identical tool Traffic Jam), uses facial recognition among other technologies to help investigators find underage sex trafficking victims in online ads. Spotlight has reportedly been used in 40,000 cases in North America, helping rescue 15,000 children and identify 17,000 traffickers (as of July 2020). On average this single platform leads to 9 child victims being identified and recovered each day across the US. Other non-governmental organizations (NGOs) also provide critical help in human trafficking cases using facial recognition by providing specialized resources to support investigations. The National Center for Missing and Exploited Children (NCMEC) has a variety of resources to assist police and district attorney's including using facial recognition technology to identify traffickers and victims (missing children) involved in human trafficking, facial reconstruction imaging for missing and deceased children, identification, and authentication of known victims of sexual exploitation images/videos, and facilitation of missing person searches and interstate traveler cases.							
sutton police department	We do not currently use FR and have no plans to use it.	No	No	Yes	Yes	No	
Templeton Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Tewksbury, Town of	Yes. We currently use FR (please answer questions 1B and 1C).	5-7 years	20-50	No	No	Yes	Yes
Topsfield Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	We need it, this is a vital tool in solving crime.
Town of Andover	We do not currently use FR but we have plans to use it.	No	No	Yes	Yes	No	
Town of Provincetown	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Townsend Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
University of Massachusetts Amherst	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Uxbridge PD	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Wakefield Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	
Warren Police Department	We do not currently use FR and have no plans to use it.	No	No	No	No	No	

Webster Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Wellesley Police Department	Yes. We currently use FR (please answer questions 1B and 1C).	Approx 3 years	20-50	No	Yes	Yes	Yes	Yes	All of our FR requests are done by outside agencies, mostly by Fusion.
Wellesley Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Wenham Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
West Brookfield Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
West Springfield Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Westminster Police Department	We do not currently use FR, but we have plans to use it.			No	No	No	No	No	
Weston Police	We do not currently use FR and have no plans to use it.			No	No	No	No	No	Personally speaking No one in Weston has used the technology, however, as a former Detective Lieutenant, for many years, in another agency, I have used the Registry of Motor Vehicles technology. With the right guidelines in place, it is extremely helpful to use in keeping our community safe.
Whitman Police Department	We do not currently use FR and have no plans to use it.			No	No	Yes	Yes	Yes	The Whitman PD requested the RMV facial recognition technology to identify several aliases used by an illegal alien who was distributing illicit narcotics.
Winchendon Ma. Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Winchester Police Dept	We do not currently use FR and have no plans to use it.			No	No	No	No	No	Used once approx. ten years ago on a sexual assault. RMV facial and 3rd party.
Woburn Police Department	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Worcester State University Police	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Worthington Police	We do not currently use FR and have no plans to use it.			No	No	No	No	No	
Wrentham Police Department	We do not currently use FR and have no plans to use it.	N/A		No	No	No	No	No	No
Yarmouth Police Department	We do not currently use FR and have no plans to use it.			No	No	Yes	Yes	No	Facial recognition is such an important tool to help detect and solve many crimes from terrorism, identity theft, fraud, sexual assault, murder and other violent crime. It is understood that facial recognition alone is not absolute and must be corroborated with other information to ensure accuracy. Restricting facial recognition will reduce public safety and increase victimization.

Appendix F
Follow-Up Survey Template

Massachusetts Special Commission on Facial Recognition
FOLLOW-UP SURVEY TO LAW ENFORCEMENT AND PROSECUTING AGENCIES

commission website: <https://frcommissionma.com/>

electronic version of survey: <https://forms.gle/VqmVYsQkAsatAzNP6>

The Massachusetts Special Commission on Facial Recognition, which was established under [Section 105 of Chapter 253 of the Acts of 2020](#), respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or *department's* use or review of facial recognition (FR) technology or FR search results **within the last three (3) years**. We ask that you please respond to this follow up survey by **December 15, 2021**.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Use of Facial Recognition

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).
2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.
3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a "trial" or temporary basis? If YES, identify the date, duration, and material details of that "trial" or temporary usage.
4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines), and, if your office or department has used different standards, describe when, why, and how your office or department has used them.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, describe:
 - A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);
 - B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);
 - C. the type of case in which facial recognition was used;
 - D. what specific software(s) was used;
 - E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);
 - F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;
 - G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;
 - H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and
 - I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.
6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.
7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?
10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?
11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?
12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?
13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?
14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

Appendix G

Follow-Up Survey Responses

Acushnet Police Department

**Massachusetts Special Commission on Facial Recognition
FOLLOW-UP SURVEY TO LAW ENFORCEMENT AND PROSECUTING AGENCIES**

commission website: <https://frcommissionma.com/>

electronic version of survey: <https://forms.gle/VqmVYsQkAsatAzNP6>

The Massachusetts Special Commission on Facial Recognition, which was established under [Section 105 of Chapter 253 of the Acts of 2020](#), respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or *department's* use or review of facial recognition (FR) technology or FR search results **within the last three (3) years**. We ask that you please respond to this follow up survey by **November 1, 2021**.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Use of Facial Recognition

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

No – to my knowledge no such request has ever been made of an outside agency.

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a "trial" or temporary basis? If YES, identify the date, duration, and material details of that "trial" or temporary usage.

On one occasion in 2017-18 we used a short lived facial recognition function within the CopLink application. Basically, we took a snap shot of a suspect on scene which then was compared to

mugshots available via Coplink in real time. No match was found.

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines), and, if your office or department has used different standards, describe when, why, and how your office or department has used them.

There were no defined standards other than we were trying to ID a drug suspect that we suspect was giving us a false ID.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, describe:

1 time, 2017-2018

- A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

No results were received

- B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

No

- C. the type of case in which facial recognition was used;

Drug possession

- D. what specific software(s) was used;

Function within CopLink

- E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

Reasonable suspicion that suspect was who he claimed to be (no ID in hand)

- F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

The search was unsuccessful.

- G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

No

- H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

No

- I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

No criminal charges arose. Suspect was present when we did the search and got no results.

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

No

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

N/A

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

None in effect at the time. None now. We haven't used since. The function is no longer available to my knowledge.

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

None, we do not use.

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

None, we do not use.

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

None, we do not use.

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

None, we do not use.

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

N/A

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

We used a rudimentary form of facial recognition on one occasion via the CopLink application for mobile phones. This was done in real time with the suspect present. The effort produced no results. We have no plans to purchase or otherwise utilize facial recognition software.

Arlington Police Department

MA Special Commission on Facial Recognition FOLLOW-UP SURVEY

The Massachusetts Special Commission on Facial Recognition, which was established under Section 105 of Chapter 253 of the Acts of 2020, respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or department's use or review of facial recognition (FR) technology or FR search results within the last three (3) years. We ask that you please respond to this follow up survey by November 1, 2021.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Email *

[REDACTED]

Respondent Contact Information

Name

[REDACTED]

Title

[REDACTED]

Organization

Arlington Police Department

Phone Number

[REDACTED]

Email Address

[REDACTED]

Use of Facial Recognition Technology

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

Yes. Years ago when the technology was new our office used it a few times to confirm suspect IDs. This was done thru the registry. I do not have exact information of the details of the inquiries, because it was years ago. Also, after speaking with DEA FTO, his task force group has used FR thru the MA Fusion Center to confirm suspect IDs.

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

NO

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a "trial" or temporary basis? If YES, identify the date, duration, and material details of that "trial" or temporary usage.

NO

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines)? If your office or department has used different standards, describe when, why, and how your office or department has used them.

We do not have a standard set of guidelines, policy or procedures.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, please answer sub-questions A-I below:

I don't have that information.

A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

From the Registry (years ago) and the MA Fusion Center.

B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

N/A

C. the type of case in which facial recognition was used;

Mainly drug cases

D. what specific software(s) was used;

Unknown

E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

Reasonable suspicion

F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

Yes

G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

Yes

H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

Yes

I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

Unknown

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

No

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

Unknown

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

We do not have a standard set of guidelines, policy or procedures.

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

None

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

We do not have a standard set of guidelines, policy or procedures.

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

We do not have a standard set of guidelines, policy or procedures.

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

We do not have a standard set of guidelines, policy or procedures.

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

Human Operator makes the judgement and then submits the photo for review.

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

No

This content is neither created nor endorsed by Google.

Google Forms

Ashby Police Department

MA Special Commission on Facial Recognition FOLLOW-UP SURVEY

The Massachusetts Special Commission on Facial Recognition, which was established under Section 105 of Chapter 253 of the Acts of 2020, respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or department's use or review of facial recognition (FR) technology or FR search results within the last three (3) years. We ask that you please respond to this follow up survey by November 1, 2021.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Email *

[REDACTED]

Respondent Contact Information

Name

[REDACTED]

Title

[REDACTED]

Organization

Ashby Police

Phone Number

[REDACTED]

Email Address

[REDACTED]

Use of Facial Recognition Technology

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

No

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or “trial” uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a “trial” or temporary basis? If YES, identify the date, duration, and material details of that “trial” or temporary usage.

No

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines)? If your office or department has used different standards, describe when, why, and how your office or department has used them.

FR not used by the agency

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, please answer sub-questions A-I below:

A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

.....

B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

.....

C. the type of case in which facial recognition was used;

.....

D. what specific software(s) was used;

.....

E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

.....

F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

.....

G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

.....

H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

.....

I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

.....

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

.....

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

.....

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

Not currently using FR

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

No FR Technology is used by Ashby Police

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

.....

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

The Department does not have FR Technology and would not likely seek in the near future.

.....

This content is neither created nor endorsed by Google.

Google Forms

Dedham Police Department

MA Special Commission on Facial Recognition FOLLOW-UP SURVEY

The Massachusetts Special Commission on Facial Recognition, which was established under Section 105 of Chapter 253 of the Acts of 2020, respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or department's use or review of facial recognition (FR) technology or FR search results within the last three (3) years. We ask that you please respond to this follow up survey by November 1, 2021.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Email *

[REDACTED]

Respondent Contact Information

Name

[REDACTED]

Title

[REDACTED]

Organization

Dedham Police Department

Phone Number

[REDACTED]

Email Address

[REDACTED]

Use of Facial Recognition Technology

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

Yes. One of our detectives has used facial recognition in two cases in the last three years, one in 2018 and one in 2020. The 6/4/2018 case was a drug investigation seeking the identity of a male distributor of narcotics and the incident on 10/It was a single request/ each time thought the State Police Fusion Center. The incidents on 9/27/2020 was a road rage and stabbing incident.

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

NO

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a "trial" or temporary basis? If YES, identify the date, duration, and material details of that "trial" or temporary usage.

NO

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines)? If your office or department has used different standards, describe when, why, and how your office or department has used them.

Until the recent changes regarding the use of Facial Recognition, we have always used the standard request forms mandated by the Mass State Police.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, please answer sub-questions A-I below:

6/4/2018; 9/27/2020

A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

Commonwealth Fusion Center

B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

No

C. the type of case in which facial recognition was used;

Narcotics case and an assault/stabbing case

D. what specific software(s) was used;

unknown

E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

reasonable suspicion

F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

Yes in the narcotics case, No in the stabbing case

G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

Search and arrest warrant

H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

Yes

I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

Yes

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

No

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

male, Hispanic, Dominican Republic

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

At the time we followed the mandates of the agency performing the facial recognition

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

None

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

N/A

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

N/A

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

N/A

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

The submitting detective decides

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

N/A

This content is neither created nor endorsed by Google.

Google Forms

Kingston Police Department

MA Special Commission on Facial Recognition FOLLOW-UP SURVEY

The Massachusetts Special Commission on Facial Recognition, which was established under Section 105 of Chapter 253 of the Acts of 2020, respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or department's use or review of facial recognition (FR) technology or FR search results within the last three (3) years. We ask that you please respond to this follow up survey by November 1, 2021.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Email *

[REDACTED]

Respondent Contact Information

Name

[REDACTED]

Title

[REDACTED]

Organization

Town of Kingston

Phone Number

[REDACTED]

Email Address

[REDACTED]

Use of Facial Recognition Technology

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

NESPIN, Report date: 02/14/20, identified suspect via associate to social media posts

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a "trial" or temporary basis? If YES, identify the date, duration, and material details of that "trial" or temporary usage.

No

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines)? If your office or department has used different standards, describe when, why, and how your office or department has used them.

None at time.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, please answer sub-questions A-I below:

02/14/2020

A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

Received form NESPIN.

B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

N/A

C. the type of case in which facial recognition was used;

Unarmed robbery

D. what specific software(s) was used;

NESPIN (unknown)

E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

NESPIN Policy/procedures

F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

Yes

G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

Yes

H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

Discovery for an ongoing case.

I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

Yes

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

No

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

Black male. The following are unknown: national origin, sexual orientation, religion, and inclusion in other protected classes

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

None at the time. Currently following new standards per Police Reform.

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

None at the time. Currently following new standards per Police Reform.

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

None at the time. Currently following new standards per Police Reform.

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

None at the time. Currently following new standards per Police Reform.

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

None at the time. Currently following new standards per Police Reform.

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

N/A, NESPIN determined quality.

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

Facial recognition has only been used one time per NESPIN suggestion/assistance in an unarmed robbery investigation.

This content is neither created nor endorsed by Google.

Google Forms

Marlborough Police Department

**Massachusetts Special Commission on Facial Recognition
FOLLOW-UP SURVEY TO LAW ENFORCEMENT AND PROSECUTING AGENCIES**

commission website: <https://frcommissionma.com/>

electronic version of survey: <https://forms.gle/VqmVYsQkAsatAzNP6>

The Massachusetts Special Commission on Facial Recognition, which was established under [Section 105 of Chapter 253 of the Acts of 2020](#), respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or *department's* use or review of facial recognition (FR) technology or FR search results **within the last three (3) years**. We ask that you please respond to this follow up survey by **November 1, 2021**.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Use of Facial Recognition

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

Yes - Commonwealth Fusion Center

05/08/2019 Request

05/08/2019 Information Returned

A photograph from bank surveillance was provided to the Fusion Center to help identify a suspect involved in fraudulent activity where she presented as another person.

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a "trial" or temporary basis? If YES, identify the date,

duration, and material details of that “trial” or temporary usage. **No**

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines), and, if your office or department has used different standards, describe when, why, and how your office or department has used them.

We do not have a formal policy on the use of facial recognition at this time.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, describe:

- A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

We received results from the Commonwealth Fusion Center. We sent them a bank surveillance picture and they returned results to us.

- B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

N/A

- C. the type of case in which facial recognition was used;

The was a fraud case that originated from St. Mary’s Credit Union. A female presented a false identification and proceeded to defraud the credit union out of 15K.

- D. what specific software(s) was used;

N/A – Commonwealth Fusion Center performed searches

- E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

N/A

- F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

[REDACTED] 05/08/2019 Yes

- G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order; **Yes – Arrest Warrant**

- H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and
Yes – presented to the clerk magistrate as part of probable cause for an arrest warrant
- I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case. **The detective's narrative indicates facial recognition was utilized. The suspect still has an open warrant in WMS for this case.**
6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.
No
7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes. **[REDACTED] 05/08/2019 Hispanic Arrest Warrant Issued**

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition? **We do not currently have formal guidelines for Facial Rec submissions.**
9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition? **Officers that have been to "Identifying the Imposter" have received training on indicators of ID Fraud.**
10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology? **We do not have any**
11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition? **We do not currently have formal guidelines for Facial Rec submissions.**
12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology? **We do not currently have formal guidelines for Facial Rec submissions.**

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?
If a photo is sent to the Commonwealth Fusion Center and/or NESPIN they determine whether the photo can be used or not.
14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here: **No**

Milton Police Department

MA Special Commission on Facial Recognition FOLLOW-UP SURVEY

The Massachusetts Special Commission on Facial Recognition, which was established under Section 105 of Chapter 253 of the Acts of 2020, respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or department's use or review of facial recognition (FR) technology or FR search results within the last three (3) years. We ask that you please respond to this follow up survey by November 1, 2021.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Email *

[REDACTED]

Respondent Contact Information

Name

Title

.....

Organization

.....

Phone Number

.....

Email Address

.....

Use of Facial Recognition Technology

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

Yes, on rare occasions detectives have. I do not have specifics before me because it was through State Police CPAC joint investigations.

.....

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a "trial" or temporary basis? If YES, identify the date, duration, and material details of that "trial" or temporary usage.

No

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines)? If your office or department has used different standards, describe when, why, and how your office or department has used them.

Law at time

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, please answer sub-questions A-I below:

.....

A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

.....

B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

.....

C. the type of case in which facial recognition was used;

.....

D. what specific software(s) was used;

.....

E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

.....

F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

.....

G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

.....

H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

.....

I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

.....

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

.....

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

.....

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

.....

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

.....

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

.....

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

.....

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

.....

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

.....

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

Very rare used. Do like thought of having the option/resources available for future.

This content is neither created nor endorsed by Google.

Google Forms

**The Massachusetts State Police Response To The
Massachusetts Special Commission on Facial Recognition
FOLLOW-UP SURVEY TO LAW ENFORCEMENT AND PROSECUTING AGENCIES**

commission website: <https://frcommissionma.com/>
electronic version of survey: <https://forms.gle/VqmVYsQkAsatAzNP6>

Use of Facial Recognition

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

Answer: Yes, the Massachusetts State Police (MSP) will initiate its own facial recognition searches in criminal investigations. MSP has also requested facial recognition searches related to criminal investigations from agencies in other states. Because G.L. c. 6, § 220 only became effective on July 1, 2021, MSP did not track its own or search requests to other state agencies until after July 1, 2021.

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or “trial” uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

Answer: Yes, The Massachusetts State Police has utilized facial recognition technology from CopLink in the past. The Massachusetts State Police began utilizing facial recognition technology from CopLink beginning in 2009. By 2020 MSP informally stopped utilizing facial recognition technology from CopLink. MSP officially stopped utilizing facial recognition technology from CopLink on January 13, 2021.

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a “trial” or temporary basis? If YES, identify the date, duration, and material details of that “trial” or temporary usage.

Answer: No.

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines), and, if your office or department has used different standards, describe when, why, and how your office or department has used them.

Answer: See attached.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, describe:
- A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);
 - B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);
 - C. the type of case in which facial recognition was used;
 - D. what specific software(s) was used;
 - E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);
 - F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;
 - G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;
 - H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and
 - I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

Answer: (A-I) Because G.L. c. 6, § 220 only became effective on July 1, 2021, MSP did not track information regarding its own searches or search requests to other state agencies until after July 1, 2021. Notwithstanding that no information was tracked prior to July 1, 2021, MSP has received one written request to utilize facial recognition technology based upon a court order. However, that request did not meet the statutory definition of a facial recognition search because the request sought to compare an image containing the face of an identified individual against the database of the registry of motor vehicles.

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

Answer: No.

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

Answer: MSP does not track information regarding a facial recognition search after the search has been completed or the request was denied.

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

Answer: See attached.

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

Answer: Face Comparison and Identification Training (FCIT)

This is a 24 hour course designed to provide the skills and knowledge to professionals from the law enforcement and intelligence communities working in the fields of face recognition and face comparison. It also provides awareness and understanding of the face comparison discipline. This training is consistent with the guidelines and recommendations outlined by the Facial Identification Scientific Working Group (FISWG).

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

Answer: See attached.

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

Answer: See attached.

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

Answer: See attached.

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

Answer: MSP submits any photo into the facial recognition system provided by the requestor, provided that all the requirements of G.L. c. 6, § 220 have been met, with the understanding that the search may not provide a result because the photo submitted is not of adequate quality to be used.

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

Answer: No.



Commonwealth Fusion Center Standard Operating Procedure

Effective Date	Number
September 27, 2019	CFC-10
Subject: CFC Use of Massachusetts Registry of Motor Vehicles Facial Recognition System for Investigative Purposes	

GENERAL

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. The Commonwealth Fusion Center (CFC) has access to the Massachusetts Registry of Motor Vehicles (MA-RMV) facial recognition system via a memorandum of agreement to support the investigative efforts of law enforcement and public safety agencies both within and outside the Commonwealth of Massachusetts.

PURPOSE

It is the purpose of this policy to provide CFC personnel with guidelines and principles for the collection, access, use, dissemination and retention of images and related information applicable to the implementation of a facial recognition (FR) program directly related to the MA-RMV facial recognition system. The requirements imposed by this policy are in addition to any policies, procedures, requirements, restrictions or directives imposed by the MA-RMV related to utilization of their facial recognition system. This policy will ensure that all CFC MA-RMV facial recognition system uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties of individuals.

All utilizations of the MA-RMV facial recognition system are for official use only.

APPLICABILITY

These guidelines apply only to the CFC's use of the MA-RMV facial recognition system in the process of supporting public safety and conducting investigations. They do not apply to, or limit other CFC or department wide activities related to the investigation or detection of unlawful conduct, the preservation of the peace and public safety, or other legitimate law enforcement activities.

PERMITTED CFC USE OF MA-RMV FACIAL RECOGNITION SYSTEM

- A. The CFC's use of the MA-RMV facial recognition system is strictly limited to law enforcement and public safety purposes only. The CFC does not perform any facial recognition services for members of the general public. The following are valid law enforcement and public safety purposes:
- Criminal investigations;
 - Crime analysis;
 - Criminal intelligence;
 - To mitigate an imminent threat to health or safety;
 - To assist in the identification of a deceased person or any individual unable to identify themselves due to incapacitation or otherwise;
 - For comparison to determine whether an individual may have obtained one or more official state driver's licenses, temporary driver's licenses, learners permits or identification cards that contain inaccurate, conflicting, false or fraudulent information;
 - To support law enforcement in critical incident responses;
 - To reduce a threat to health, homeland security or public safety.
- B. CFC personnel will only utilize the MA-RMV facial recognition system to seek or retain information that:
- a. Is based on a criminal predicate or threat to public safety; or
 - b. Is based upon reasonable suspicion that an individual or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or criminal activity; or

- c. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
 - d. Is useful in the investigative process, crime analysis or situational assessment reports for the administration of criminal justice and public safety.
- C. CFC personnel will not utilize the MA-RMV facial recognition system to seek or retain information about:
 - a. Individuals or organizations solely on the basis of their religious, political, social views or activities; or
 - b. An individual's or organization's participation in a particular non-criminal organization or lawful event; or
 - c. An individual's age, race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual.
- D. Using or requesting use of the MA-RMV facial recognition system for personal use is strictly prohibited and considered employee misconduct as well as a violation of this policy. Unauthorized access and dissemination of driver license images for unofficial purposes constitutes a violation of the Drivers Privacy Protection Act (DPPA) 18 U.S.C. § 2721.
- E. The CFC does not connect the MA-RMV facial recognition system to any external interface; including any system that would perform live video surveillance.

PROCEDURES FOR CFC USE OF MA-RMV FACIAL RECOGNITION SYSTEM

- A. Trained CFC authorized users may utilize the MA-RMV facial recognition system pursuant to this policy for both internal matters and to assist external law enforcement and public safety agencies. These users shall only consist of CFC personnel that have been trained by and authorized for access to the MA-RMV facial recognition system by the MA-RMV. Furthermore, authorized access to

the MA-RMV facial recognition system will be granted only to CFC personnel whose positions and job duties require such access. User names and passwords to the MA-RMV facial recognition system are not transferable, must not be shared, and must be kept confidential.

- a. CFC personnel who receive a request to utilize the MA-RMV facial recognition system must take appropriate steps to ensure that the requestor is either a Department member or an appropriately credentialed law enforcement or public safety agent.

Requests must be sent from an official government email address unless exigent circumstances exist in which case a request may be submitted by a verified law enforcement officer or public safety agent from an identified telephone number. However, the nature of the exigency shall be noted in the appropriate CFC database.

- b. CFC personnel shall log all requests in the appropriate CFC database to include the following information:
 - 1) Date and time of request
 - 2) Name and agency of requester
 - 3) Contact information for requester
 - 4) Requester's case number, file number, or incident number
 - 5) Reason for query
 - 6) Requestor's probe image if one is provided
 - 7) Results of query
 - 8) The exigency if one existed
 - 9) All other significant actions taken
- c. Subject of interest probe images may only be submitted by verified law enforcement or public safety personnel.
- d. CFC personnel who receive a request to utilize the MA-RMV facial recognition system must review the submitted photograph (angle of photo, clarity of photo, level of detail) to determine its suitability. Photographs that are not suitable will not be submitted for analysis via the MA-RMV facial recognition system and the requestor will be notified.
- e. For photographs submitted for analysis via the MA-RMV facial recognition system, any results that appear to be an investigative lead produced by the MA-RMV facial recognition system may be provided, pursuant to paragraph (g) below, to the requestor for their review along with the following statement:

The Commonwealth Fusion Center is providing this information as a result of a search utilizing the MA-

RMV facial recognition system. The results are NOT being provided as a form of positive identification of any subject, they are considered advisory in nature as an investigative lead only and do NOT establish probable cause, without further investigation. Any possible connection between the information provided and any identified individual must be determined and validated through further investigation or corroboration which shall be the sole responsibility of the requestor.

If the request was made by telephone in compliance with this policy pursuant to an exigency, the above statement shall initially be made to the requester verbally over the telephone followed by a written notification from the respective CFC personnel.

- f. When appropriate, CFC personnel may share information resulting from the use of the MA-RMV facial recognition system, with other law enforcement or public safety agencies in order to further the CFC's law enforcement and public safety missions.
 - g. If CFC personnel develop an investigative lead via utilization of the MA-RMV facial recognition system, said personnel shall not disclose any screenshot of the MA-RMV facial recognition system to the requestor. Rather, CFC personnel shall forward an RMV-1 printout of each potential match to the requestor. CFC personnel shall also notify the requestor to contact the Fraud Identification Unit for further assistance.
- B. The CFC will retain and disseminate records of requests, photographs, and any other information submitted internally for a MA-RMV facial recognition system query based on the type of file the submission corresponds to. For example, retention and dissemination of facial recognition information produced from a search of information located within an intelligence file will be treated in the same manner as an intelligence file. Information obtained during the course of a criminal investigation will be located within the investigative record and retained and disseminated accordingly.
- C. Any procedures performed by CFC personnel pursuant to the submission of information from an external source (e.g. local police department) for a MA-RMV facial recognition system query will be logged pursuant to CFC protocols. Aside from CFC activity logs, CFC personnel are not required to maintain information or develop an internal case file for information submitted from external sources when the CFC's sole involvement is the performance of a MA-RMV facial recognition system query. Dissemination of facial recognition

analysis information produced by the CFC for an external source will follow CFC procedures based on the category of information produced. Information will not be released to anyone other than verified law enforcement or public safety officials.

- D. The CFC's facial recognition search information will not be sold, published, exchanged, or disclosed to commercial or private entities/individuals unless required by law. Nor will it be disclosed to unauthorized individuals or for unauthorized purposes.

COMPLAINTS, MISCONDUCT & AUDITS

Personnel will report violations or suspected violations of this directive to their supervisor who will determine the appropriate course of conduct or disciplinary action. The respective supervisor shall immediately report violations or suspected violations related to utilization of the MA-RMV facial recognition system to the MA-RMV.

The CFC will maintain an audit trail of information logged as a result of CFC personnel's use of the MA-RMV facial recognition system.

RESERVATIONS

These guidelines are set forth solely for the purpose of internal CFC guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the Commonwealth Fusion Center, Massachusetts State Police, or the Commonwealth of Massachusetts.

Promulgated By:

Norwood Police Department

MA Special Commission on Facial Recognition FOLLOW-UP SURVEY

The Massachusetts Special Commission on Facial Recognition, which was established under Section 105 of Chapter 253 of the Acts of 2020, respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or department's use or review of facial recognition (FR) technology or FR search results within the last three (3) years. We ask that you please respond to this follow up survey by November 1, 2021.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Email *

[REDACTED]

Respondent Contact Information

Name

[REDACTED]

Title

[REDACTED]

Organization

Norwood Police Department

Phone Number

[REDACTED]

Email Address

[REDACTED]

Use of Facial Recognition Technology

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

Yes. Massachusetts State Police Fusion Center, NESPIN and the Rhode Island State Police Fusion Center. We've used these agencies from 2014 to present. We've asked for any and all identification information on suspects of various crimes.

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or “trial” uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a “trial” or temporary basis? If YES, identify the date, duration, and material details of that “trial” or temporary usage.

No

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines)? If your office or department has used different standards, describe when, why, and how your office or department has used them.

The Norwood Police Department has implemented all the standards of probable cause, reasonable suspicion and exigent circumstances in each different investigation. Some cases we already have probable cause on a suspect, but will request facial recognition to be done to develop more probable cause (“icing on the cake if you will”) and to identify any other identities the suspect may have (as in identity fraud/imposter investigations). Some investigations we will have a photo of a suspect, but we do not know their true identity so we have reasonable suspicion to request facial recognition to help identify a possible suspect that we can later use to investigate further to corroborate the identity and involvement in the crime as provided through facial recognition. We would certainly authorize the use of facial recognition technology/software in an investigation where exigency (murder, terrorism, kidnapping, sexual assault, suicidal person, etc.) was a factor, but thankfully we have not had to do so based on exigency as of yet.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, please answer sub-questions A-I below:

- 1.) November 2016 (3 investigations)
 - 2.) February 2017 (5 investigations)
 - 3.) April 2017 (1 investigation)
 - 4.) October 2017 (1 investigation)
 - 5.) November 2017 (2 investigations)
 - 6.) February 2018 (1 investigation)
 - 7.) August 2018 (1 investigation)
 - 8.) January 2018 (1 investigation)
 - 9.) September 2018 (1 investigation)
 - 10.) December 2018 (2 investigations)
 - 11.) June 2019 (1 investigations)
 - 12.) February 2020 (2 investigations)
 - 13.) March 2020 (1 investigations)
 - 14.) April 2020 (2 investigations)
 - 15.) May 2020 (2 investigations)
 - 16.) August 2020 (2 investigations)
 - 17.) October 2020 (1 investigation)
-

A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

Every search we've submitted was to another agency/organization such as the MSP Fusion Center, the RISP Fusion Center, NESPIN or the Puerto Rican Special Arrest or Warrant and Extradition Units. Here are where we sent each request as follows:

- 1.) 3 sent to MSP Fusion Center
- 2.) 5 sent to NESPIN.
- 3.) 1 sent to NESPIN
- 4.) 1 sent to MSP Fusion Center
- 5.) 1 sent to NESPIN and MSP Fusion Center, 1 sent to NESPIN
- 6.) 1 sent to MSP Fusion Center
- 7.) 1 sent to MSP Fusion Center and RISP Fusion Center
- 8.) 1 sent to MSP Fusion Center
- 9.) 1 sent to Central Florida Information Exchange (CFIX)
- 10.) 2 sent to MSP Fusion Center
- 11.) 1 sent to MSP Fusion Center
- 12.) 2 sent to MSP Fusion Center
- 13.) 1 sent to NESPIN
- 14.) 2 sent to NESPIN
- 15.) 2 sent to MSP Fusion Center
- 16.) 2 sent to MSP Fusion Center
- 17.) 1 sent to HSI/NYNJ HIDTA and NESPIN and 1 sent to MSP Fusion Center

B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

We requested each and every search on our own accord, no other agency or department has requested us to conduct or request facial recognition on their behalf.

C. the type of case in which facial recognition was used;

- 1.) Narcotics, Firearms, Identity Fraud/Imposter
- 2.) Narcotics, Larceny, Identity Fraud/Imposter
- 3.) Identity Fraud/Imposter
- 4.) Larceny Scam
- 5.) Narcotics, Benefit Fraud, Insurance Fraud, Identity Fraud/Imposter
- 6.) Narcotics, Identity Fraud/Imposter
- 7.) Identity Fraud/Imposter
- 8.) Narcotics, Identity Fraud/Imposter
- 9.) Elder Scam/Larceny
- 10.) Narcotics, Benefit Fraud, Identity Fraud/Imposter
- 11.) Narcotics, Identity Fraud/Imposter
- 12.) Identity Fraud/Imposter
- 13.) Identity Fraud/Imposter
- 14.) Narcotics, Benefit Fraud, Identity Fraud/Imposter
- 15.) Identity Fraud/Imposter/Larceny of MV, Failure to ID on MV Stop/Suspended License
- 16.) Narcotics, Identity Fraud/Imposter, Annoying and Accosting Sexually
- 17.) Narcotics, Identity Fraud/Imposter

D. what specific software(s) was used;

The Facial Recognition Software that the MSP Fusion Center, the RISP Fusion Center and NESPIN utilize.

E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

All of the above (Probable cause, Reasonable Suspicion and Exigent Circumstances) are considered as a standard used by the investigator or supervisor to authorize the request and use of facial recognition. We will never authorize or utilize facial recognition without an official ongoing investigation into criminal activity or exigent circumstance.

F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

On most of the investigations the use of facial recognition has helped to either develop and or confirm the identity of the suspect or has helped to identify other fraudulent identities the suspect had. Unfortunately, many of our Identity Fraud/Imposter investigations that originated from Narcotics investigations has shown suspects to have multiple stolen identities through the Registry of Motor Vehicles. Many of these same suspects use these stolen identities to defraud the Commonwealth of Massachusetts Division of Transitional Assistance (DTA) as well.

G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

Yes. The use of facial recognition requests/searches did result in criminal charges filed (summons), arrests and various types of arrest and/or search warrants being sought against a number of suspects. On one case in particular which involved an elder scam, the investigating detective was able to use the suspect's own social media photo to submit to facial recognition to already confirm the identity the detective had developed and suspected. The detective was able to obtain an NCIC warrant and extradite the suspect back to Massachusetts from Florida to face the criminal charges. On another case, this same detective again used the suspect's own social media and bank surveillance photos to confirm the identity the detective had developed and suspected. That suspect later confessed and made full restitution to the victim as a result.

H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

Yes, many of our facial recognition requests are involved in official investigations and are therefore disclosed in our police reports and saved digitally into a folder. These can later be easily found and provided to the defense and prosecution as part of discovery prior to court proceedings.

I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

Yes, provided through the discovery process at the District or Superior Court levels.

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

No, never for the Norwood Police Department. If the photo is of poor quality the agency that is conducting the facial recognition search for us will tell us and we will not proceed. If the matches are not of sufficient numerical scale, it is considered not a match and the information will not be pursued. The MSP Fusion Center always has a disclaimer in their result email of: "The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation."

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

Most suspects were Males only approximately four were female. Some suspects were African American some suspects were Hispanic and some suspects were Caucasian. Many suspects involved in our identity fraud/imposter investigations are foreign nationals from the Dominican Republic utilizing stolen Puerto Rican citizen's identities. The sexual orientation, religion or inclusion in any other protected classes were not known about any of the suspects.

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

The Norwood Police Department has no rules or guidelines for the use of facial recognition.

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

The Norwood Police Department does not have any software to conduct facial recognition, we always request another agency such as the MSP Fusion Center or NESPIN to conduct the facial recognition search for us. Therefore, we do not provide any training or certification to investigators on facial recognition. In regard to oversight, the Norwood Police Department always has a supervisor review the officer or detective's investigation and reports and consult with the department prosecutor before and after facial recognition was requested on any particular investigation. All facial recognition results were then added to the incident or arrest reports and into evidence to be used for court and available through the discovery process.

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

The Norwood Police Department has a longstanding working relationship with all law enforcement agencies/entities (MSP, NESPIN, HIDTA, HSI, FBI, CBP, DHS) and would reach out to them through email or over the phone to request their facial recognition services. There is no official written procurement policy or procedure.

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

The Norwood Police Department has no policies in place for reporting regarding facial recognition.

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

The Norwood Police Department has no protocols in place relating to privacy, civil rights, due process and other legal protections relating to the use of facial recognition.

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

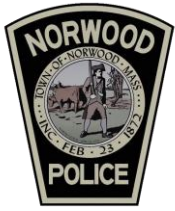
The Norwood Police Department will first consult with the agency that we will be requesting the facial recognition search of and ask if the photo we are submitting is of sufficient quality. Once submitted, there is a standard numbered grading system utilized with facial recognition technology results from 0-100.

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

Facial Recognition Technology is a very important and necessary tool law enforcement has to use in a wide array of investigations. It IS NOT probable cause. It is just one of many items an investigator has and may need to investigate a suspect. It has been proven to lead investigators to the correct suspects and furthered important investigations that otherwise could not have been conducted effectively without it. Used correctly and judiciously, it again is a great tool and is needed.

This content is neither created nor endorsed by Google.

Google Forms



Norwood Police Department

Facial Recognition Requests/Investigations

Case # [REDACTED]

On 10/05/17 a Norwood resident filed a Larceny Under \$250 report. The victim was interested in purchasing a laptop through Facebook Marketplace, and the victim communicated with the seller, Facebook username "Molly Marry Brown". The victim and the seller agreed to meet in Norwood Center to exchange \$150 cash for the laptop. The victim gave the seller \$150 as the seller was seated in the passenger seat of his friend's car. The car sped off prior to the victim taking possession of the laptop.

The victim reported that he recognized the seller by the photos on seller's Facebook page. The victim showed a screen shot of one of the seller's Facebook photos. I was able to access the seller's Facebook page through open source social media. I shared some of photos of "Molly Marry Brown" from his Facebook page with the MA Fusion Center for assistance in facial recognition. The Fusion Center found a "potential match" to REDACTED of Stoughton, MA. I called [REDACTED] in for an interview. He acknowledged that he was "Molly Marry Brown" and agreed to reimburse the victim prior to criminal charges being applied for (at the victim's request).

Case # [REDACTED]

A 78yr old Norwood resident fell victim to a scam over several months in 2018. The victim believed he was paying for attorney fees to help him get out of a time-share agreement in Florida. The victim transferred over \$57,000 from his bank account to two separate accounts. Norwood Police applied for and were issued search warrants for the receiving bank accounts which identified the account holders. REDACTED was the lone holder of one of the accounts and he provided a Florida identification and his Social Security card to open that account. Norwood Police also acquired bank surveillance images from several transactions that REDACTED completed at various bank branches in Florida. I shared some of the bank surveillance images with the Central Florida Intelligence Exchange (CFIX) for assistance in facial recognition. CFIX identified a "potential match" to REDACTED.

In 2019, REDACTED was indicted by a Norfolk County grand jury for Larceny over \$1200, and ultimately pled guilty.

Case # [REDACTED]

In May of 2019, Norwood Police detectives began a narcotics investigation into narcotics dealing in Norwood. The suspected narcotics dealer was surveilled and a photo was taken of the unidentified dealer with a high powered long range surveillance camera. The surveillance photo was later submitted to the MSP Fusion Center on 6/14/2019 for facial recognition. The search was conducted by an Intelligence Analyst and she replied that the program had uncovered a possible match of REDACTED. REDACTED's email also contained the following disclaimer/warning: The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation. Independent probable cause developed and later search warrants were obtained and executed with the Boston Police Drug Control Unit. A very large amount of narcotics and money were seized.

Case # [REDACTED]
[REDACTED]

In the early hours on the 12am-8am shift, on Thursday, May 24th, 2020 Officer [REDACTED] was conducting traffic enforcement on Route 1 in Norwood. He stopped a vehicle for a motor vehicle infraction. The driver kept providing incorrect spellings of his name and different dates of birth thus not identifying himself as required by law. As much information was taken down and the driver was allowed to leave to go to work down the street at Home Market Foods on Morgan Drive in Norwood, but not before a good quality photo was taken of him. The photo was then submitted by [REDACTED] to the MSP Fusion Center and a positive result came back as REDACTED. The MSP Lieutenant that sent the results spoke to [REDACTED] over the phone and cautioned that the return may or may not be the suspect. The photo of REDACTED's driver's license matched that of the photo taken by [REDACTED] on the traffic stop. Officers then went to speak to [REDACTED] now knowing his probable true identity, but he had not shown up for work and told his manager he had to leave for a family emergency. He was summonsed for Operation After License Suspension, Failure to Identify Self on MV Stop, and various motor vehicle violations. The circumstance of this case would allow an officer to arrest a motorist, but [REDACTED] took a less intrusive approach. The case is still pending at Dedham District Court.

Case # [REDACTED]
[REDACTED]

On Thursday, May 14th, 2020 [REDACTED] took a report for a stolen U-Haul truck that was rented with a counterfeit Connecticut driver's license under the name of [REDACTED]. [REDACTED] submitted the image from the counterfeit Connecticut drivers' license to the MSP Fusion Center and a possible match came back as REDACTED of Boston. The photo of REDACTED's Massachusetts driver's license matched that of the photo on the counterfeit Connecticut driver's license. The MSP Fusion Center email stated: The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation. A subsequent investigation revealed the stolen U-Haul to be recovered by the Boston Police right around the corner from REDACTED's residence. He was subsequently charged with Failure to Return/Conceal Leased Property and Identity Fraud and defaulted, thus a warrant for his arrest has issued.

Case # [REDACTED]
[REDACTED]

On Wednesday, 4/1/2020, in the early hours of the morning [REDACTED] was conducting surveillance of the USPS Mailboxes at the Norwood Post Office on Central Street. Norwood had been recently hit with a string of numerous "mailbox fishing" incidents where thousands of dollars was stolen from victims. [REDACTED] observed a vehicle park nearby and individuals go up to the mailboxes and start to attempt to steal mail. The vehicle and five individuals were stopped and investigated. Burglarious instruments were discovered in the vehicle used to conduct mailbox fishing to steal mail. Information and good quality photos were also taken of each suspect. After further investigation, one individual subsequently provided a false identity. His photo was submitted to the MSP Fusion Center by [REDACTED] and a positive result was returned as REDACTED. The MSP Fusion Center email stated: The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through

further investigation. The photo on REDACTED's license matched the photo of the individual taken by the vehicle at the time of the investigation. The five individuals were all summonsed for Possession of Burglary Tools/Instruments, Attempt to Commit a Crime (Larceny) and Conspiracy. The cases remain open at Dedham District and Norfolk County Juvenile Courts.

Case # [REDACTED] – Narcotics, multiple ID Frauds

On November 2017, an NPD officer conducted a car stop following a suspected drug transaction. During that interaction, he identified REDACTED#1 and REDACTED#2 as the occupants of the vehicle. No arrests were made during that stop. Once the officer returned to the station, he learned that REDACTED#1 was one of the Impostors from prior cases. Following the stop, he requested MASP Fusion Center run facial recognition on both individuals. I learned that REDACTED #1 had multiple identities using different names and biographical information on them. Specifically, REDACTED #1 had 12 names, 6 dates of birth, 4 social security numbers, and at least 4 Driver's licenses. Due to the fact that REDACTED #1 had a Puerto Rican Social Security number, the officer also contacted the Puerto Rican Warrant and Extradition Unit and asked for a query into the identity as well. I learned that the real REDACTED#1, with PR issued documents looked completely different from our suspect. REDACTED #1 had been arrested numerous times under the assumed names and we were able to locate this information through the use of facial recognition applied by the Fusion Centers.

REDACTED #2

During the car stop above, the officer also found indicators that led him to believe that REDACTED #2 was an Impostor. REDACTED #2 had difficulty answering simple questions of who he was and where he was from. Following the stop, I asked the Puerto Rico Warrant and Extradition team for all information regarding REDACTED#2, he learned that the True Identity Holder and our Impostor were two completely different people.

Narcotics investigation

On Nov 2016 an NPD Officer received information regarding a criminal organization selling narcotics in Norwood. CI provided the names of [REDACTED] and [REDACTED] as two individuals who he/she personally bought drugs from. CI provided us with the suspects Facebook account information which contained several pictures of them. After confirming the Facebook Accounts with the CI, the officer submitted their photographs to MSP Fusion Center and positively identified both REDACTED and REDACTED. The drug transaction was unsuccessful but REDACTED #1 was later arrested numerous times for drug offenses as well as several firearms offenses.

Case # [REDACTED] – Identity Fraud, Benefits Fraud, Narcotics, Firearms.

On Dec 24, 2018, NPD responded to REDACTED 's address with DCF for a wellness check on a minor. During this interaction, ██████████ recognized REDACTED as someone we had identified as an "Impostor" (Foreign National living under the assumed identity of an US Citizen). ██████████ attempted to obtain a true identity for Piris. During the course of our investigation we submitted REDACTED picture as well as social security number to MA Fusion Center, PR Fusion Center. The results showed multiple people using the same name and social security numbers, one out of Puerto Rico, and two out of Massachusetts. The person we had in custody was an Impostor, a second impostor REDACTED #2 had been arrested and deported as well. REDACTED #1 from Norwood had been arrested by ██████████ during a joint investigation between NORPAC, Middlesex County Drug Task Force and State Police. On his BOP there are several trafficking charges as well as failure to stop for police, intimidation. He served four years in State prison under that assumed name.

While investigating REDACTED #1 we identified a second individual using the same biographical information. Following a facial rec and additional investigation we learned that REDACTED#2 had assumed REDACTED 's identity as well and had been arrested and removed from the US.

Case # ██████████ – Narcotics Investigation

On 11/23/16 REDACTED was arrested for Possession to Distribute Class B (Cocaine). During the course of the drug investigation, CI provided information that a individual known to him/her as ██████████ was selling Cocaine to several Norwood residents. We made several attempts to identify the individual during the course of our investigation. At some point during the course of our investigation, we obtained photographs of REDACTED and submitted them to MSP Fusion Center. The result of the search yielded an individual that looked similar to our suspect but was determined it was not REDACTED. Therefore no action was taken against the individual in question.

Case # ██████████ – MV Stop/MV Violations

REDACTED was arrested following a car stop by ██████████. During our interaction with these individuals I observed several indicators that we were dealing with an Impostor using a fraudulent identity. I contacted MSP Fusion Center and requested a facial rec. run on both individuals. The results from MA were negative. I also contacted Puerto Rico Warrant and Extradition Unit and requested all information regarding these individuals including photos of them. During the course of my investigation I learned that REDACTED from MA had a completely different picture from REDACTED from PR. Additionally, both individuals were incarcerated in MA and PR during the same timeframe. I later located the True Identity Holder and spoke with him. He said that his identity had been stolen while he was in Federal Prison in Puerto Rico and that several people have been using his information. At the time of his arrest, REDACTED was on a GPS monitor for a shooting out of Boston. He had several narcotics violations as well as Aggravated ABDW w/ serious bodily injury, Use without Authority, Possession of firearm, Dist Class B.

Case # [REDACTED] – MV Case

REDACTED was identified following a motor vehicle stop in January of 2020. Through our investigations using facial rec. we were able to identify that REDACTED had two driver's license under two different names. He had obtained driver's licenses in Florida under the assumed name and we were able to see this through facial rec. and other investigative tools.

Case # [REDACTED] - ID Fraud

There were two individuals in Norwood using the same information. Facial rec. was conducted on one of them by NESPIN using a RI DOC photo with no results. Susp. Identity fraud.

Case # [REDACTED] – Narcotics

DEA/FBI/NORPAC search warrant on a stash house in Norwood led to the arrest of REDACTED. Both parties were removed from the country following the 2015 case. In 2017 I saw both individuals at Walmart in Walpole. Facial Rec from HSI identified REDACTED as REDACTED, a Dominican National.

Theft

REDACTED was charged with stealing used tires at a local dealership. I was contacted by the case officer and asked to run facial rec under the suspicion that he was an impostor. No matches.

Pittsfield Police Department
Massachusetts Special Commission on Facial Recognition
FOLLOW-UP SURVEY TO LAW ENFORCEMENT AND PROSECUTING AGENCIES
commission website: <https://frcommissionma.com/>
electronic version of survey: <https://forms.gle/VqmVYsQkAsatAzNP6>

The Massachusetts Special Commission on Facial Recognition, which was established under [Section 105 of Chapter 253 of the Acts of 2020](#), respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or *department's* use or review of facial recognition (FR) technology or FR search results **within the last three (3) years**. We ask that you please respond to this follow up survey by **November 1, 2021**.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Use of Facial Recognition

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

Yes, as part of a narcotics investigation approximately three years ago, members of the Pittsfield Police Department Drug Unit utilized Clearview in an attempt to identify an individual who was selling narcotics. Investigators used a photograph from the targets open Facebook page to gain his identity from a news article. No law enforcement action was conducted.

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No. It was a trial period.

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a “trial” or temporary basis? If YES, identify the date, duration, and material details of that “trial” or temporary usage.

Yes. (see answer #1 for the details)

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines), and, if your office or department has used different standards, describe when, why, and how your office or department has used them.

The information obtained was only to identify a potential target who was distributing narcotics and believed to be in possession of firearms. No law enforcement action was taken.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, describe:
- A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

Directly

- B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

No

- C. the type of case in which facial recognition was used;

Narcotics/Firearms

- D. what specific software(s) was used;

Clearview AI

- E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

Informational purposes only

- F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

Yes, from a news article

- G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

No

- H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

No

- I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

Not applicable

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

No

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

Not applicable

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?
9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?
10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?
11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?
12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?
13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?
14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

Southwick Police Department

From: [REDACTED]
Sent: Friday, December 10, 2021 1:19 PM
To: [REDACTED]
Subject: Re: Important: Facial Recognition Commission Follow-Up Survey

[REDACTED],

I received the attached survey, but I am not aware of the Southwick Police utilizing or inquiring about the use of Facial recognition over the last three years.

Stoneham Police Department

MA Special Commission on Facial Recognition FOLLOW-UP SURVEY

The Massachusetts Special Commission on Facial Recognition, which was established under Section 105 of Chapter 253 of the Acts of 2020, respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or department's use or review of facial recognition (FR) technology or FR search results within the last three (3) years. We ask that you please respond to this follow up survey by November 1, 2021.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Email *

[REDACTED]

Respondent Contact Information

Name

[REDACTED]

Title

[REDACTED]

Organization

Stoneham Police Department

Phone Number

[REDACTED]

Email Address

[REDACTED]

Use of Facial Recognition Technology

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

No

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a "trial" or temporary basis? If YES, identify the date, duration, and material details of that "trial" or temporary usage.

No

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines)? If your office or department has used different standards, describe when, why, and how your office or department has used them.

None

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, please answer sub-questions A-I below:

May 2019

A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

Search conducted by CrimeDex and Mount Pleasant Police Department, WI

B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

No

C. the type of case in which facial recognition was used;

Identity theft

D. what specific software(s) was used;

Unknown

E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

None

F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

Yes

G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

Stoneham Police Department - no. Another agency - unknown

H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

Stoneham Police Department - no. Another agency - unknown

I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

Stoneham Police Department - no. Another agency - unknown

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

No

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

N/A

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

None exist as it is a product not used by the department.

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

None

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

None exist as it is a product not used by the department

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

None

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

None exist as it is a produce not used by the department

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

N/A

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

The instance of facial recognition reported to the Commission involved an identity theft investigation that originated in Stoneham, with other crimes committed in Georgia. The SPD detective conducting the investigation posted the suspect photo on CrimeDex, an online network used by private industry fraud investigators, loss prevention, and law enforcement for fraud and other white collar crime cases. A detective from a police agency in WI and someone from CrimeDex ran the photo through a software program and provided the SPD the possible social media accounts of a suspect. These checks were unsolicited by the SPD. The SPD detective was able to view the suspects Instagram page and found in a post the suspect wearing the same clothes during a fraudulent ATM withdrawal. This information was passed along to a police department in Georgia that was conducting a similar investigation. No charges resulted from the Stoneham investigation.

This content is neither created nor endorsed by Google.

Google Forms

commission website: <https://frcommissionma.com/>
electronic version of survey: <https://forms.gle/VqmVYsQkAsatAzNP6>

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

Use of Facial Recognition

- Yes. NESPIN.**

06/19/2019
06/17/2019
05/19/2019
03/13/2019
07/18/2018
07/18/2018
06/19/2018
06/19/2018
06/07/2018
06/07/2018
05/19/2017
04/2017
07/05/2017
09/10/2017
09/13/2017
09/13/2017
09/13/2017

09/13/2017

02/13/18

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or “trial” uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a “trial” or temporary basis? If YES, identify the date, duration, and material details of that “trial” or temporary usage.

No

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines), and, if your office or department has used different standards, describe when, why, and how your office or department has used them.

We do not have a formal policy on the use of facial recognition at this time.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, describe:
- A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);
Question 1 has all dates and requests. Our requests are sent by Officers, to NESPIN, and the search is conducted by them. Our Officers receive an e-mail with results from NESPIN.
 - B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);
N/A
 - C. the type of case in which facial recognition was used;
All aforementioned requests were used in narcotics based investigations
 - D. what specific software(s) was used;
N/A – NESPIN performed searches

E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);
N/A

F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

████████████████████	06/19/2019	Yes
██████████	06/17/2019	Yes
██████████████	05/19/2019	Yes
Unspecified photo	03/13/2019	No
██████████████	07/18/2018	Yes
██████████████	07/18/2018	Yes
████████████████████	06/19/2018	Yes
██████████████████	06/19/2018	Yes
██████████	06/07/2018	Yes
██████████	06/07/2018	Yes
██████████████	05/19/2017	Yes
██████████████	04/2017	Yes
██████████████	07/05/2017	No
██████████	09/10/2017	Yes
██████████████	09/13/2017	Yes
██████████████	09/13/2017	Yes
██████████	09/13/2017	Yes
██████████████	09/13/2017	Yes
██████████████	02/13/18	Yes

G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

████████████████████	06/19/2019	Yes
██████████	06/17/2019	Yes
██████████████	05/19/2019	Yes
Unspecified photo	03/13/2019	No
██████████████	07/18/2018	Yes
██████████████	07/18/2018	Yes
████████████████████	06/19/2018	Yes
██████████████████	06/19/2018	Yes
██████████	06/07/2018	Yes
██████████	06/07/2018	Yes
██████████████	05/19/2017	Yes
██████████████	04/2017	Yes
██████████████	07/05/2017	No
██████████	09/10/2017	Yes
██████████████	09/13/2017	Yes

████████████████████	09/13/2017	Yes
██████████	09/13/2017	Yes
████████████████████	09/13/2017	Yes
████████████████████	02/13/18	Yes

H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

██	06/19/2019	No
████████████████████	06/17/2019	No
████████████████████████████████	05/19/2019	No (NH License)
████████████████████████████████	03/13/2019	No
████████████████████████████████	07/18/2018	No
████████████████████████████████	07/18/2018	No
██	06/19/2018	No
██	06/19/2018	No
████████████████████	06/07/2018	No
████████████████████	06/07/2018	No
████████████████████████████████	05/19/2017	No
████████████████████████████████	04/2017	Yes
████████████████████████████████	07/05/2017	No
████████████████████	09/10/2017	No
████████████████████████████████	09/13/2017	Yes
████████████████████████████████	09/13/2017	No
████████████████████	09/13/2017	Yes
████████████████████████████████	09/13/2017	No
████████████████████	02/13/18	No

I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

No

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

████████████████████	05/19/2019	Male, Hispanic,
████████████████████████████████	06/19/2018	Male, Hispanic
████████████████████	04/2017	Male, Hispanic
████████████████████████████████	09/13/2017	Female, Hispanic
████████████████████	09/13/2017	Male, Hispanic

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition? **We do not currently have formal guidelines for Facial Rec submissions.**
9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition? **Officers that have been to “Identifying the Imposter” have received training on indicators of ID Fraud.**
10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?
11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition? **We do not currently have formal guidelines for Facial Rec submissions.**
12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?
We do not currently have formal guidelines for Facial Rec submissions.
13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as ‘poor quality’ or does a human operator make this judgment)?
If a photo is sent to NESPIN, they determine whether the photo can be used or not.
14. If there is any additional information you would like the Commission to know about your office or department’s use or review of facial recognition technology or search results, please provide it here: **NA**

Wellesley Police Department

MA Special Commission on Facial Recognition FOLLOW-UP SURVEY

The Massachusetts Special Commission on Facial Recognition, which was established under Section 105 of Chapter 253 of the Acts of 2020, respectfully requests that each office and department in your purview, including any employees, agents, or third parties assisting that office or department, answer the following questions and provide the requested information relating to your office or department's use or review of facial recognition (FR) technology or FR search results within the last three (3) years. We ask that you please respond to this follow up survey by November 1, 2021.

Your office is receiving this follow-up survey because your office or department previously indicated that it has used or reviewed FR technology or search results.

For purposes of this survey, FR is defined as an automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head, or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that FR shall not include the use of search terms to sort images in a database. For purposes of this survey, FR does NOT include common FR applications used by a person to gain access or log onto that person's electronic device, e.g., logging onto a smart phone.

Email *

[REDACTED]

Respondent Contact Information

Name

[REDACTED]

Title

[REDACTED]

Organization

Wellesley Police

Phone Number

[REDACTED]

Email Address

[REDACTED]

Use of Facial Recognition Technology

1. Has your office or department, or any agent or employee of your office or department, ever requested that a law enforcement, prosecuting, or other governmental agency, including, but not limited to, the State Police or Registry of Motor Vehicles, conduct a facial recognition search in connection with a criminal investigation? If YES, identify the agency(ies), date, duration, and material details of request(s).

Yes. Requests have gone through the RMV and Coplink. We do not have the ability to easily track each case usage at this time.

2. Has your office or department ever entered into a contractual or other relationship, whether formal or informal, with a company for the lease, use, possession, or other provision of facial recognition technology? This does not include requests to law enforcement or prosecuting agencies (covered by question 1) or temporary or "trial" uses of facial recognition technology (covered by question 3). If YES, identify the company(ies), date, duration, and material details of that contract or relationship.

No

3. Has your office or department, or any agent or employee of your office or department, ever tested or used facial recognition technology on a "trial" or temporary basis? If YES, identify the date, duration, and material details of that "trial" or temporary usage.

Yes. Motorola/Vigilant. March 2019.

4. What standard(s), if any, has your office or department used to determine whether to authorize or request a facial recognition search (e.g., legal standards, including probable cause, reasonable suspicion, exigent circumstances, or other internal standards or guidelines)? If your office or department has used different standards, describe when, why, and how your office or department has used them.

Generally speaking, the department has utilized Facial Recognition on a reasonable suspicion or probable cause basis. In most cases I am aware of, a photo of the suspect (PC) in the act of committing a crime (or close time proximity) has been obtained and investigators are seeking a possible ID to further the case.

Search Details

5. Provide the approximate date of each facial recognition search conducted or receipt of facial recognition search results by your office or department. For each search listed, please answer sub-questions A-I below:

Unable to track each individual case with our present RMS.

A. whether your office or department conducted the search directly or received results from another office, department, agency, or organization (and if so, who);

.....

B. whether your office or department conducted the search at the request of another office, department, agency, or organization (and if so, who);

.....

C. the type of case in which facial recognition was used;

.....

D. what specific software(s) was used;

.....

E. the standard used to approve or authorize the use (e.g., probable cause, reasonable suspicion, exigent circumstances, or other internal standard or guideline);

Reasonable Suspicion at times, Probable Cause most of the time.

.....

F. whether the results of the facial recognition search helped to confirm or identify a suspect or person of interest in a criminal investigation;

.....

G. whether the results of the facial recognition search were used by your office or other law enforcement agencies to obtain a search warrant, arrest warrant, or other court order;

.....

H. whether the results of the facial recognition search were submitted into evidence or otherwise used in any deposition, pleading, hearing, proceeding, or trial; and

.....

I. whether the existence and results of the facial recognition search were disclosed and/or provided to the defendant in that case.

.....

6. Are you aware of any individual(s) who was falsely identified by facial recognition as used or reviewed by your office, and based on that false identification, was subsequently stopped, searched, interrogated, or arrested by law enforcement? Please provide details.

None that I am aware of. There is no way to accurately track usage with our present RMS.

.....

7. For instances where the use of facial recognition has led to an arrest, provide any available information on the arrestees' gender, race, color, national origin, sexual orientation, religion, and inclusion in other protected classes.

.....

Training, Rules & Policies

8. What rules and guidelines did and/or does your office or department follow for the use or review of facial recognition?

Use is outsourced at this time, we only receive potential candidates from outside agencies.

9. What training, certification, and oversight did and/or does your office or department provide to your employees and agents regarding the use or review of facial recognition?

Some have completed a basic Facial ID class, but the work is outsourced to larger agencies as noted.

10. What procurement policies and procedures did and/or does your office or department have in place relating to the use and acquirement of facial recognition technology?

We do not use it internally at this time.

11. What reporting policies did and/or do your office or department have in place relating to the use or review of facial recognition?

It is noted in the report narrative/case file if utilized.

12. What protocols does your office or department have in place relating to privacy, civil rights, due process, and other legal protections relating to the use of facial recognition technology?

All present legal standards are followed.

13. How does your office or department determine whether a photo is of adequate quality to be used as an input to a facial recognition system (e.g., does the system automatically reject some photos as 'poor quality' or does a human operator make this judgment)?

The photos are outsourced-we do not perform that internally.

14. If there is any additional information you would like the Commission to know about your office or department's use or review of facial recognition technology or search results, please provide it here:

This content is neither created nor endorsed by Google.

Google Forms

Appendix H
*Department of State Police Policy and Procedure “Use of Facial
Recognition Technology”*



Department of State Police

General Order

Effective Date: December 6, 2021	Number: INV-19
Subject: Use of Facial Recognition Technology	

General

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce fraud, prevent individuals from becoming victims of identity theft, reduce an imminent threat to health or public safety, and help in the identification of persons unable to identify themselves or deceased persons.

The Department has access to the Massachusetts Registry of Motor Vehicles (MA-RMV) facial recognition system via a memorandum of agreement to support the investigative efforts of law enforcement within and outside the Commonwealth of Massachusetts. The Department does not authorize the use of any other facial recognition technology. The use of other facial recognition technology is prohibited without prior approval from the Office of the Superintendent.

Purpose

The purpose of this policy is to provide Department personnel with guidelines and principles related to utilization of the MA-RMV facial recognition system. The requirements imposed by this policy are in addition to any policies, procedures, requirements, restrictions, or directives imposed by the MA-RMV related to utilization of their facial recognition system. All utilization of the MA-RMV facial recognition system is for official use only.

Definitions

Biometric Data: Computerized data relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of such person, including, but not limited to, facial recognition, fingerprints, palm veins, deoxyribonucleic acid, palm prints, hand geometry or iris recognition.

Biometric Surveillance System: Any computer software that performs facial recognition or other remote biometric recognition.

Facial Recognition: An automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head or body, that uses characteristics of an individual's face, head or body to infer emotion, associations, activities or the location of an individual; provided, however, that "facial recognition" shall not include the use of search terms to sort images in a database.

Subject:	Number:
Use of Facial Recognition Technology	INV-19

Definitions,
continued

Facial Recognition Search: A computer search using facial recognition to attempt to identify an unidentified person by comparing an image containing the face of the unidentified person to a set of images of identified persons; provided, however, that a set of images shall not include moving images or video data.

Facial Recognition Software: A category of biometric software that maps an individual's facial features mathematically and stores the data as a faceprint.

Match: For the purposes of this policy only, situations where investigative follow up has determined that probable cause exists to believe that two photos are in fact one in the same person.

Applicability

These guidelines apply to the Department's use of the MA-RMV facial recognition system.

These guidelines do not apply to the Department's acquisition, possession, and use of personal electronic devices, such as cell phones or tablets that utilize facial recognition technology for the sole purpose of user authentication.

These guidelines do not apply to the Department's acquisition, possession, and use of automated video or image redaction software; provided, that such software does not have the capability of performing facial recognition or other remote biometric recognition.

These guidelines do not limit the Department's ability to receive evidence related to the investigation of a crime derived from a biometric surveillance system; provided, that the use of a biometric surveillance system was not knowingly solicited by or obtained with the assistance of a public agency or any public official in violation of any section or subsection of this policy or relevant law.

Subject:	Number:
Use of Facial Recognition Technology	INV-19

Permitted Use

Any law enforcement agency requesting a facial recognition search within the MA-RMV Facial Recognition System shall only do so through a written request submitted to the Department. All requests received shall be forwarded to the Department's Fraud Identification Unit.

A law enforcement agency may request such a facial recognition search for the following purposes:

- To execute an order, issued by a court or justice authorized to issue warrants in criminal cases, based upon specific and articulable facts and reasonable inferences therefrom that provide reasonable grounds to believe that the information sought would be relevant and material to an ongoing criminal investigation or to mitigate a substantial risk of harm to any individual or group of people; or
- Without an order to identify a deceased person or if the law enforcement agency reasonably believes that an emergency involving substantial risk of harm to any individual or group of people requires the performance of a facial recognition search without delay. Any emergency request shall be narrowly tailored to address the emergency and shall document the factual basis for believing that an emergency requires the performance of a facial recognition search without delay.
- This subsection shall not apply to the department of state police when performing investigatory functions related to the issuance of identification documents by the registrar of motor vehicles.

Procedures for Use of MA-RMV Facial Recognition System

Only trained and authorized users assigned to the Department's Fraud Identification Unit may utilize the MA-RMV facial recognition system.

User names and passwords to the MA-RMV facial recognition system are not transferable, must not be shared, and must be kept confidential.

Fraud Identification Unit personnel who receive a request to utilize the MA-RMV facial recognition system must review the submitted photograph to determine its suitability for comparison purposes. Photographs that are not suitable will not be submitted for analysis via the MA-RMV facial recognition system and the requestor will be notified. The Department prohibits the use of facial recognition technology to analyze composite images.

Department personnel shall log all law enforcement requests for searches related to the MA-RMV facial recognition system in the appropriate Department database to include the following information:

- A copy of any written request made for a facial recognition search;
- A copy of any court order, if applicable;
- Date and time of the request;

Subject:	Number:
Use of Facial Recognition Technology	INV-19

**Procedures for
Use of MA-
RMV Facial
Recognition
System,
continued**

- Number of matches returned, if any;
- The database searched;
- Name and position of the requesting individual and employing law enforcement agency;
- The reason for the request, including, but not limited to, any underlying suspected crime;
- The entity to which the request was submitted;
- Data detailing the individual characteristics included in the facial recognition request;
- Requester's case number, file number, or incident number;
- Such documentation shall not be a public record, except as provided by applicable state law; and
- The Department shall report such documentation quarterly to the Executive Office of Public Safety and Security (EOPSS).

**Reporting to
EOPSS**

The Department shall document each facial recognition search performed and shall provide such documentation quarterly to the Executive Office of Public Safety and Security.

Such documentation shall include:

- A copy of any written request made for a facial recognition search;
- The date and time of the request;
- The number of matches returned, if any;
- The database searched;
- The name and position of the requesting individual and employing law enforcement agency;
- The reason for the request, including, but not limited to, any underlying suspected crime;
- The entity to which the request was submitted; and
- Data detailing the individual characteristics included in the facial recognition request.

Reservations

These guidelines are set forth solely for the purpose of internal Department guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and legal prerogatives of the Massachusetts State Police, or the Commonwealth of Massachusetts.

Promulgated By: **Christopher S. Mason, Colonel/Superintendent**