

COMMONWEALTH OF MASSACHUSETTS

Suffolk, ss.

Superior Court

AMERICAN CIVIL LIBERTIES UNION OF  
MASSACHUSETTS, INC.

Plaintiff,

v.

MASSACHUSETTS DEPARTMENT OF  
TRANSPORTATION and STEPHANIE  
POLLACK, in her Official Capacity as the  
SECRETARY AND CHIEF EXECUTIVE  
OFFICER OF THE MASSACHUSETTS  
DEPARTMENT OF TRANSPORTATION,

Defendants.

Civil Action No. 1984CV02193 D

COMPLAINT

RECEIVED

JUL 10 2019

SUPERIOR COURT-CIVIL  
MICHAEL JOSEPH DONOVAN  
CLERK/MAGISTRATE

INTRODUCTION

1. Plaintiff American Civil Liberties Union of Massachusetts, Inc. (“ACLUM”) seeks public records from Defendant Massachusetts Department of Transportation (“MassDOT”) revealing how and to what extent MassDOT uses and shares access to its photograph database of millions of Massachusetts residents for face surveillance purposes.

2. In 2006, MassDOT made its database containing the photographs of every person who has applied for a state-issued ID (“RMV database”)—nearly ten million persons at the time—available to local, state, and federal law enforcement agencies for face surveillance purposes. MassDOT has shared this database in secret and without regulation.

3. Face surveillance is an automated or semi-automated process which attempts to identify persons based on their facial characteristics.

4. Many public spaces are now under the constant watch of publicly and privately owned cameras accessible to government agencies. Combined with face surveillance technology,

these cameras enable governments to track and identify their residents from the moment they leave their front door to the moment they return home thanks, in part, to those residents doing nothing more than obtaining a driver's license or photo ID through the Registry of Motor Vehicles ("RMV").

5. Massachusetts, in the past, has used technology to monitor people's political activities,<sup>1</sup> and recent advancements in face surveillance technology permit government agencies to monitor the location, movement, and habits of law-abiding residents with a scope not before seen. Coinciding developments of data storage technology permit agencies to store this information indefinitely, creating the potential to keep detailed records tracking the daily routines of millions of people, including information about how those activities evolve over time.

6. This monitoring poses an unprecedented threat to civil rights and civil liberties, including basic First and Fourth Amendment freedoms.

7. As the U.S. Supreme Court recently held, under the Fourth Amendment, "an individual maintains a legitimate expectation of privacy in the record of his physical movements." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). Our Supreme Judicial Court this year emphasized that "society's expectation has been that law enforcement could not secretly and instantly identify a person's real-time physical location at will." *Commonwealth v. Almonor*, 482

---

<sup>1</sup> In 2012, ACLUM released *Policing Dissent*, a report documenting the following:

- (1) The Boston Regional Intelligence Center ("BRIC") had, for years, tracked and created criminal intelligence reports of lawful political activity of peace groups and local leaders, including Veterans for Peace, Stop the Wars Coalition, and Code Pink.
- (2) The Boston Police Department recorded peaceful protests and events using handheld and stationary cameras, and retained those recordings for unknown periods of time, despite the fact that no illegal activity occurred or resulted from the event recorded.

ACLUM, *Policing Dissent: Police Surveillance of Lawful Political Activity in Boston* (2012), <https://www.aclum.org/sites/default/files/wp-content/uploads/2015/06/reports-policing-dissent.pdf>.

Mass. 35, 46 (2019).

8. Yet face surveillance technology can enable the government to use real-time data to track and store the location, routines, and habits of its residents absent regulation or public disclosure. And unlike the tracking at issue in *Carpenter* and *Almonor*, face surveillance does not arise from an individual's arguably voluntary act of engaging a third party to provide cell phone service, but instead from the quite involuntary fact of having a face.

9. In addition to federal and state constitutional protections against unreasonable searches and seizures, the First Amendment protects the right to dissent. It protects our freedom to engage in political protest, intimate and expressive association, speech, and the free exercise of religion without undue interference by the government.

10. The unregulated use of face surveillance can jeopardize those protections because, if broadly applied in public spaces, it can amount to requiring every person, including every person who engages in political dissent, to carry and display a personal photo identification card at all times. Indeed, the face surveillance technology company Geofeedia advertised that law enforcement used its technology to identify and arrest protestors with outstanding warrants during the Baltimore protests surrounding the death of Freddie Gray.<sup>2</sup> The advertisement notes that its archive data can be used to arrest and prosecute as many of the protestors as possible.<sup>3</sup>

11. What is more, research shows significant shortcomings in the accuracy of face surveillance technology, especially as it relates to distinguishing among genders and within non-white races, which can lead to harmful misidentifications. For example, researchers Joy Buolamwini, from MIT Media Lab, and Timnit Gebru, from Microsoft Research, found that the

---

<sup>2</sup> Geofeedia, Case Study: Baltimore County PD, [https://www.aclunc.org/docs/20161011\\_geofeedia\\_baltimore\\_case\\_study.pdf](https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf).

<sup>3</sup> *Id.*

error rate of three leading face surveillance programs in determining the gender of lighter-skinned, male faces ranged from 0 to 0.8 percent.<sup>4</sup> Yet, for those same programs, the error rate when determining the gender of darker-skinned, female faces ranged from 20.8 to 34.7 percent.<sup>5</sup>

12. Public accountability for face surveillance technology is critical given both its potential reach and the depth of its flaws. Yet the public has little, if any, insight into how this technology is being used in the Commonwealth and what, if any, safeguards are in place.

13. To bridge this knowledge gap, ACLUM sent MassDOT two public records requests. The first, sent over four months ago on February 20, 2019, sought, *inter alia*, communications and policies about the use of face surveillance at the agency as well as any audits indicating the effectiveness of any face surveillance program actually in use. The second, dated April 24, 2019, sought documents governing the sharing of information contained in the RMV database with, and records showing the number of times access to the database has been given to, public or private persons, entities, or companies outside the agency.

14. MassDOT has ignored these requests. To date, MassDOT has not responded to either request, nor has it produced any of the requested records.

15. Due to its failure to comply with the public records law, MassDOT's use of face surveillance technology, and the nature and extent of its coordination with federal, state, municipal, and/or private agencies and actors around the use of face surveillance technology, remain unclear. At this critical juncture where the development of technology is outpacing government regulation, an informed public is more important than ever in shaping how the government will use face

---

<sup>4</sup> J. Buolamwini & T. Gebru, *Gender Shades*, Proceedings of Machine Learning Research 81:1-15 (2018), <https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf>.

<sup>5</sup> *Id.*



surveillance technology in the future.

### JURISDICTION AND VENUE

16. Jurisdiction and venue are proper in this Court pursuant to G.L. c. 66, § 10A(c).

### PARTIES

17. Plaintiff ACLUM is a Massachusetts nonprofit corporation with a principal place of business in Boston, Massachusetts.

18. Defendant MassDOT is an agency of the Commonwealth of Massachusetts and a custodian of the records Plaintiff seeks. Its principal place of business is in Boston.

19. Defendant Stephanie Pollack is the Secretary and Chief Executive Officer of MassDOT and a custodian of the records Plaintiff seeks. She is being sued in her official capacity. Her usual place of employment is in Boston.

### FACTS

#### *Face Surveillance Technology's Inherent Flaws*

20. Face surveillance is an automated or semi-automated process that assists in identifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, or that logs characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of an individual.<sup>6</sup> Facial recognition is a type of face surveillance technology, which employs a face detection algorithm to create templates of people's faces, and then compares those templates against one another to look for matches. These searches can be performed on a one-to-one basis or a one-to-many basis. In the first case, a template is compared to another template to determine whether the templates match.

---

<sup>6</sup> An Act Establishing a Moratorium on Face Recognition and Other Remote Biometric Surveillance Systems, S.B. 1385, 191st General Court of MA (2019).

In the second case, a template is compared to a number of templates to determine whether a match exists. In all of these cases, the algorithms are “taught” how to “see” using large datasets of images, which “train” the algorithm how to distinguish faces. Likewise, in all of these cases, algorithms can be programmed and reprogrammed, often at the user end, to perform identifications at varying accuracy rates.

21. Face surveillance technology has demonstrated significant errors. For example, it is much more likely to misidentify people with darker skin tones, young people, and women. These misidentifications can lead to wrongful arrests, unwarranted surveillance, and inaccurate records maintained by law enforcement agencies that erroneously involve law-abiding citizens in the criminal justice system.

22. According to the Buolamwini and Gebru study, a factor causing this misidentification is the overrepresentation of white and male faces in the dataset used to train the algorithms that animate face recognition systems.<sup>7</sup> Studying one dataset that was used to train a face recognition algorithm, the researchers found that the set of facial images therein was 77.5 percent male and 83.5 percent white.

23. In a real-life example of the harm that can be caused by face surveillance technology inaccuracies, a Brown University senior recently made news after Sri Lankan authorities erroneously included her photo, found using face surveillance software, among images of the suspects wanted for the 2019 Easter bombing. Police issued a statement acknowledging the

---

<sup>7</sup> J. Buolamwini & T. Gebru, *Gender Shades*, Proceedings of Machine Learning Research 81:1-15 (2018), <https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf>.

mistake, but the student received numerous death threats due to the error.<sup>8</sup>

24. Here in Massachusetts, the RMV's own system misidentified a Natick resident in 2011, resulting in the revocation of his license for two weeks. To get it restored, he was required to attend a hearing in Boston and provide copies of his birth certificate and social security card.<sup>9</sup>

#### *MassDOT's Facial Surveillance Technology*

25. The RMV, a department of MassDOT, is responsible for processing and issuing state-approved photograph identification cards to Massachusetts residents, including driver's licenses.

26. As part of this function, the RMV photographs residents when they apply for a driver's license or photo ID. These photographs are entered into the RMV database on the date of application. *See* Ex. 1, FMCSA 2005 Grant Application-Fraud Protection-Facial Recognition Technology. To ACLUM's knowledge, residents are not given notice of their photograph's inclusion in a database shared with non-RMV entities, much less the option to consent or object to its inclusion.<sup>10</sup>

27. In 2006, the RMV announced to law enforcement agencies that it had acquired face surveillance technology that could be employed against its database, thereby enabling those agencies to use and search the database's photos for surveillance purposes. *See* Ex. 2, October 2006 letter from Anne Collins, RMV Registrar. The RMV database contained 9.5 million images

---

<sup>8</sup> Jeremy Fox, *Brown University student mistakenly identified as Sri Lanka bombing suspect*, The Boston Globe (April 28, 2019), <https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html>.

<sup>9</sup> Meghan Irons, *Caught in a Dragnet*, The Boston Globe (July 17, 2011), [http://archive.boston.com/news/local/massachusetts/articles/2011/07/17/man\\_sues\\_registry\\_after\\_license\\_mistakenly\\_revoked/?page=1](http://archive.boston.com/news/local/massachusetts/articles/2011/07/17/man_sues_registry_after_license_mistakenly_revoked/?page=1).

<sup>10</sup> In our public records request dated February 20, 2019, ALCUM asked for records relating to any public process of debate about any face surveillance product or service.

in 2006. *See id.*

28. MassDOT purchased this technology with the help of a \$250,000 grant from the U.S. Department of Transportation. The stated purpose for the technology was for license fraud detection. According to MassDOT's application, the total system cost \$2,879,832.50 and was implemented over four years. *See* Ex. 1, FMCSA 2005 Grant Application.

29. A 2008 Massachusetts State Police internal policy memorandum related to RMV database face surveillance stated that searches against the RMV database require only that "[a]ll inquiries must be related to an ongoing criminal investigation." *See* Ex. 3, Department of State Police Superintendent's Memo, February 21, 2008. There is no stated requirement that law enforcement agencies show probable cause or even reasonable suspicion to obtain this information. *See id.*

30. The RMV additionally entered into agreements with the FBI and multiple municipal law enforcement agencies to allow the agencies to access "personal and confidential information protected by federal Drive Privacy Protection Act (18 U.S.C. § 2721 et seq.)," which includes its photo database. *See, e.g.,* Ex. 4, Agreements for Access to Records and Data Maintained by the Registry of Motor Vehicles for the Brookline Police Department and FBI Boston. These agreements do not provide details as to what types of data are shared or for what specific purposes they may be used. Instead, the agreements vaguely state that data may only be used for a "permitted" reason and in "carrying out the official functions of [the law enforcement] agency."

31. Because MassDOT has failed to comply with the public records law to produce the requested records, ACLUM does not know whether MassDOT has entered into any additional agreements for access to its database or face surveillance technology or whether any of these

agreements contain newer terms to keep pace with the rapidly evolving and increasingly invasive technology.

*ACLUM's Public Records Requests*

32. No Massachusetts law expressly regulates the use of face surveillance or any other type of biometric tracking technology. Likewise, no federal law expressly regulates the use of this technology. Thus, state agencies have been left to self-regulate their use of face surveillance.

33. This renders MassDOT's production of responsive documents the only means of understanding how this technology and its use have affected the civil rights and civil liberties of Massachusetts residents.

34. To that end, on February 20, 2019, ACLUM submitted a written public records request under G.L. c. 66, § 10 ("February Request") to MassDOT for documents related to the agency's use of face surveillance technology, including, but not limited to, records related to searches performed by the RMV of its driver's license database and any manuals, training materials, or policies governing the use of the technology. A copy of the February Request is attached as Exhibit 5.

35. On March 22, 2019, ACLUM contacted MassDOT Records Access Officer ("RAO") William J. Doyle to inquire as to when it would receive a response. *See* Ex. 5, February Request and Correspondence.

36. On March 25, 2019, RAO Doyle erroneously referred ACLUM to a March 2019 response to a separate records request made by ACLUM in September 2018.<sup>11</sup> That same day,

---

<sup>11</sup> This complaint does not relate to the September 2018 public records request to which MassDOT responded in March 2019. That request related to memoranda of understanding and non-disclosure agreements between the RMV and law enforcement agencies, documents distinct from those sought by the requests at issue in this matter.

ACLUM responded to RAO Doyle via email that the February Request is distinct from the September 2018 request. ACLUM submitted an additional copy of the February Request and informed MassDOT that they had yet to provide a response. *See* Ex. 5, February Request and Correspondence.

37. On April 11, 2019, ACLUM again emailed RAO Doyle asking when a response could be expected. *See* Ex. 5, February Request and Correspondence.

38. ACLUM has received no further communication from defendants related to the February Request.

39. On April 24, 2019, ACLUM submitted a written public records request under G.L. c. 66, § 10 (“April Request”) to MassDOT for documents related to the agency’s sharing of information with other state and local agencies, federal agencies, and private actors. This request again informed MassDOT that it had yet to respond to the February Request. A copy of the April Request is attached as Exhibit 6.

40. On April 24, 2019, the same day that the April Request was submitted, defendants sent to ACLUM a notice that the request had been received. *See* Ex. 6, April Request and Notice.

41. Since that date, ACLUM has received no substantive response, documents, or other communication from defendants regarding either the February Request or the April Request.

#### CLAIMS FOR RELIEF

##### *Count I: Violation of G.L. c. 66, § 10*

42. ACLUM incorporates by reference and re-alleges all of the allegations in the preceding paragraphs.

43. The Massachusetts Public Records Law (“MPRL”), G.L. c. 66, § 10, strongly favors disclosure by creating a presumption that all government records are public records.

44. Under the MPRL, defendants were required to respond to ACLUM's request within ten business days, to conduct an adequate search for responsive documents, and to demonstrate the application of any exemptions. G.L. c. 66, § 10(b).

45. Defendants have custody of public records requested by ACLUM.

46. Defendants failed to provide a timely response to ACLUM's request. More than four months after the February Request and two months after the April Request, ACLUM has received no documents in response to its requests.

47. On information and belief, defendants have failed to conduct an adequate search with regard to each part of ACLUM's request.

48. Defendants' actions violate G.L. c. 66, § 10.

*Count II: Declaratory Judgment*

49. ACLUM incorporates by reference and re-alleges all of the allegations in the preceding paragraphs.

50. There is an actual controversy between ACLUM and defendants regarding the production of requested records.

51. Pursuant to G.L. c. 231A and the MPRL, ACLUM is entitled to a declaration that the records it requests are public records within the meaning of G.L. c. 66, § 10, that their release is required by law, and that defendants have no right to withhold such records.

PRAYER FOR RELIEF

**WHEREFORE**, the Plaintiff requests that this Court:

1. Issue a declaratory judgment that the records ACLUM has requested are public records within the meaning of G.L., c. 66, § 10, and that MassDOT has no right to withhold such records;



2. Enter a permanent injunction requiring MassDOT to disclose, at no cost to ACLUM, all of the records ACLUM has requested;
3. Award ACLUM its costs and attorneys' fees in bringing this action; and
4. Grant such other relief as the Court deems just and proper.

By its attorneys,



Matthew R. Segal (BBO #654489)  
Jessie Rossman (BBO #670685)  
Jessica Lewis (BBO #704229)  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION OF MASSACHUSETTS, INC.  
211 Congress Street  
Boston, MA 02110  
(617) 482-3170

Robert A. Skinner (BBO #567862)  
S. Susan Zhu (BBO #695984)  
Scott Grannemann (BBO #699955)  
ROPES & GRAY LLP  
Prudential Tower  
800 Boylston Street  
Boston, MA 02199  
(617) 951-7000

# **EXHIBIT 1**

## **FMCSA Grant Approval**

### ***Proposal: Fraud Prevention – Facial Recognition Technology- \$250,000***

The attached CDL Grant Proposal meets OMB Requirements and will substantially improve the integrity and effectiveness of the Commercial Driver's License Program in Massachusetts.

This proposal will address fraud which is one of the 2005 CDL Program Priorities. The MA RMV has identified and initiated legal action on fraudulent activities in the past and seeks to obtain the tools necessary to prevent fraudulent activities in the future. This funding would serve to prevent compromising the integrity of the Commercial Driver's License Program. The MA RMV is committed to preventing fraud as demonstrated by their commitment of additional state resources to this program.

The project will further enhance the RMV attempts to reduce the an individual from attempting to gain a fraudulent license, however the funding requested does not seem proportional to the population of CDL licensed drivers.

Richard R. Bates, Division Administrator – Massachusetts





U.S. Department  
of Transportation

Federal Motor Carrier  
Safety Administration

## Commercial Drivers License Program

The \_\_\_\_\_ Massachusetts Registry of Motor Vehicles \_\_\_\_\_ (State Lead Agency) hereby applies to the Federal Motor Carrier Safety Administration for a Federal grant authorized in Title XII of the Commercial Motor Vehicle Safety Act of 1986 (P.L. 99-570) and subsequent amendments thereto to enhance a Commercial Drivers License Program as described in this application.

- ☐ The State Agency plans to carry out the implementation of a Commercial Drivers License Program during Federal fiscal year (FY) \_\_\_\_\_ as described in the attached plan.
- ☒ The State Agency plans to carry out special projects of the Commercial Drivers License Program as described in the attached plan.

The Federal share will not exceed 80 percent of the total participating costs, unless otherwise indicated herein, incurred in performing the effort described in the attached State Plan. The State agrees to submit vouchers for the reimbursement of funds expended.

Kimberly Hinden

(Typed Name)

Registry of Motor Vehicles

(Organizational Unit)

(Signature)

P. O. Box 55889

(Address or P.O. Box)

Registrar

(Title)

Boston, MA 02205

(City, State & Zip Code)

May 11, 2005

(Date)

617-351-9000

(Phone Number)

The collection of this information is authorized under the provisions of P.L. 97-424; P.L. 99-570; 49 U.S.C. 31101-31104 and P.L. 105-178.

Public reporting for this collection of information is estimated to be 30 minutes per response, including the time for reviewing instructions and completing and reviewing the collection of information. All responses to this collection of information are mandatory, and will be provided confidentiality to the extent allowed by law. Notwithstanding any other provision of law, no person is required to respond to nor shall a person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a current valid OMB Control Number. The valid OMB Control Number for this information collection is 2126-0010. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: Information Collection Clearance Officer, Federal Motor Carrier Safety Administration, MC-MBI, U.S. Department of Transportation, Washington, D.C. 20590.

**FMCSA Grant Application – Fraud Prevention – Facial Recognition Technology**

The Massachusetts Registry of Motor Vehicles (RMV) hereby applies to the FMCSA for a portion of funding, (\$250,000), toward the purchase and implementation of facial recognition technology to be used in RMV daily business operations.

MA has 4,634,521 active licensed drivers in the state, of which 155,204 are licensed as Commercial Drivers. There are currently 2,626,873 driver's licenses in renewal status, not necessarily active.

Long term goals for improving the MA CDL program include:

- Continue to review and evaluate MA CDL program with an eye toward increasing security screening
- Improving customer service
- Expanding and improving on-line processes to provide the most secure and efficient system to customers
- Continue to explore technology opportunities and solutions with Federal partners to expand and improve ways of communicating electronically, in an effort to create a secure processing system for all involved; specifically with regard to exchanging information and image files
- Continue to build and implement an information system to incorporate all CDL license functions, CMV enforcement functions, and court functions

Examples of processes that are in place to ensure coordination between all parts of the CDL program (Licensing, Enforcement and Courts):

- The Massachusetts Registry of Motor Vehicles currently has the electronic capacity to process administrative per se and chemical test refusals from law enforcement agencies through CJIS links and the Office of Alcohol Testing.
- The RMV can also provide images and text back through that system for police and court prosecutors. The "missing link" continues to be the lack of automation within the courts.
- The RMV Chief Technology Officer is involved in planning and committee meetings with Criminal History Systems Board, Information Technology Division and Court personnel to attempt to identify and establish a solution to this problem.

The last compliance review at the MA RMV revealed the following issues which needed to be addressed. Following each issue, is the progress which has been made to date to correct the identified issue:

**CDL Compliance Review Issues – Progress to Date      April 2005**  
**Federal & State Requirements**

CDL Fingerprinting – TSA	Project successfully completed and implemented to date
School Bus Endorsement – “S” designation	Major complications in adding this endorsement to 15-year old system. Paper knowledge testing to begin last week in May. Will be completed by 9/30/05
Driving Records Request – CDL Holders	Accomplished in conjunction with AAMVA with PDPS process using unique identifier – major problem: specs not yet received from AAMV
Notification of CMV violations to home state	Part of ACD working group convened by IT staff – working with AAMVA -project on-going – All CDL violations already electronically transferred to state of record
Notification of all traffic violations to home state	Same as above
FMCSA Revocation Periods – OUI – CTR – Admin Per Se	Part of ACD working group – dependent upon AAMVA compliance and specifications
State Revocation Periods OUI – CTR – Admin Per Se	Legislation submitting by RMV attorneys to Governor’s office for filing; have been advised that filing will take place in the next few weeks with the legislature
CDL Hardship Licenses	Massachusetts does not issue CDL hardship licenses
CDLIS Reporting and Record Check Requirements	Project Implementation successfully completed May 18, 2005
Immediate Threat Status	The MA RMV Registrar currently has the authority to implement this, and is now done through posting on CDLIS

**Problem/ Need Statement**

In light of recent arrests at the MA RMV for licensing fraud, the agency has worked closely with (its previous Secretariat), the Executive Office of Public Safety, (EOPS), to explore business solutions to curb fraud. If unchecked, license fraud rears its head in many devastating directions: identity fraud, underage drinking, licensing of undocumented aliens, licensing of unqualified and dangerous drivers, to name a few potential problem areas.

After many months of meetings with and demonstrations from the company who currently produces MA licenses and identification cards, the RMV has received the support and an agreement from EOPS for some funds to purchase and implement facial recognition technology at the MA RMV.

This technology is part of a comprehensive strategy to support the notion of one license, one identity, as well as to ensure that dangerous drivers, who are often the perpetrators of license fraud, are eliminated from the licensed driving population.

The end result of these efforts will be a reduction in the potential numbers of accidents caused by erroneously licensed passenger and commercial vehicle drivers.

As license sanctions and identity requirements have become more strict over the past few years, there has been an increasing number of incidents of fraud perpetrated to obtain a license in the first place. Convictions and arrests that may not previously have resulted in loss of license, now may mean the loss of livelihood and license for commercial drivers and Hazmat carriers. For someone whose adult life has been spent employed primarily as a truck driver, these consequences may lead that driver facing loss of license to attempt to obtain a license fraudulently, or to try to transfer their revoked or suspended license from another state, before the court conviction is recorded and recognized.

**Objective**

The implementation of facial recognition technology will identify attempts at license fraud that involve:

- 1) an individual with two or more licenses under different names
- 2) different individuals holding the same license
- 3) attempts to alter signatures and facial features

The RMV wants to incorporate facial recognition technology into its daily business operations, believing that better upfront validation (which should occur with fraudulent document training and document authentication), along with production of a secure license, (new release in September, 2004), in combination with facial recognition technology will result in a truly secure licensing process. None of these solutions alone would enable the RMV to make that claim of security. But combined, these solutions can make a huge difference in the fight against fraud.



While no technology alone can combat this enormous threat, a comprehensive solution, carefully planned, can stop licensing fraud. If even one CDL holder, particularly one with an “H” endorsement, is stopped from skirting the laws and legitimate licensing issue, then the MA CDL program will have been improved, and public safety impacted (by keeping this driver off the road).

While the RMV is currently examining the purchase and implementation strategy which will be used to procure Facial Recognition technology, the RMV has been given cost estimates for implementation, services and purchase over a four-year time period.

While the funding from EOPS will not cover the entire cost of implementation of Facial Recognition technology completely, the RMV is currently considering what amount it can budget, and is seeking other funding assistance to procure this technology. Hence this request for a portion of the total \$2,879,832.50 cost for a four-year implementation strategy. While imaging each license and permit applicant for facial recognition purposes can begin immediately, and those images can be matched one at a time against the entire current RMV database, a long-term strategy is needed in order to “scrub” the existing licensing database and that population who will not be coming in “new” or for renewal until their license expiration in five years or less.

The overall goal is to decrease the numbers of licensees who currently have, or attempt to gain, a fraudulent license. In addition, the RMV is in the process of redefining its Special Investigation unit, and establishing a direct link with state police special investigators, since both parties will need to investigate the records and people turned up as suspicious by the facial recognition technology.

### **Project Description**

The RMV will develop a comprehensive business plan that incorporates document authentication technology, staff training, an on-line document verification system and facial recognition technology toward the end goal of establishing that every MA licensed driver, whether Commercial or passenger vehicle, has the legitimate right to be licensed and has one identity, and one license.

The facial recognition part of this plan works like this: the RMV is already positioned for facial recognition because its current license production vendor has a special software that it uses at every one of the RMV capture stations in the branch offices. This is where each person's photograph is taken and their signature is digitized, along with their photo in the license production process. For facial recognition to work, every photograph has to be placed and cropped specifically; RMV photos have been taken in that particular manner for the last four years. Photos not in this format will need to be prepared from the Registry's database of 7,261,394 images of licensed Massachusetts drivers.

As each person comes into the RMV to be licensed, first, all of their identity documents will be verified, then they will be photographed, regardless of whether they will actually receive a license or not. This means that if it is determined that a person is attempting to perpetrate fraud, both their documents and photograph have been captured and stored, and can be retrieved for an investigation.

At night, when all of the images captured that day are batched and sent to license production, every image is run through facial recognition software, that seeks to match every submitted image to one that is already in the database. Any questionable applicants or matches that appear problematic are again batched, removed from production, and returned to the RMV for examination.

The RMV will have their internal special investigation unit review these returned files, in order to identify any administrative anomalies, such as name change, twins, incompatible image structure, and the remaining images will be turned over to a state police investigative unit for further investigation, potentially arrest and maybe prosecution, dependent on the outcome of the investigation. It is estimated that the RMV will return approximately 500-600 images each night for next day examination, requiring full-time staff for the purpose of clearing or referring these images. The internal RMV investigator will gather all of the relevant driver history and other information useful to a police investigation, prior to turning the files over.

### **Timeline**

<b>Activity</b>	<b>Responsible Party</b>	<b>Date for Completion</b>
Establish and convene procurement team to create RFR and/or determine whether contract can be sole-sourced	RMV legal staff , Deputy Registrar Erin Deveney and Chief Fiscal Officer Mary Ellen Kelley	June 30, 2005
Begin procurement process, select company qualified from which to purchase facial recognition system and services	Mary Ellen Kelley and Procurement Team	July 30, 2005
Decide customization (options) and integration of Facial Recognition with existing IT systems	John Fuller, Chief of IT in conjunction with all impacted managers including Lorraine Lague and Deputy Registrar Rachel Madden	August 15, 2005

Activity	Responsible Party	Date for Completion
Decide whether you want any other agency to be able to have access to your enrolled facial recognition images	Registrar and other high-level secretariat staff should meet with law enforcement agency officials and determine this issue	August 15, 2005
Once decision above is made, decide HOW you want any other agency to be able to have access to your enrolled facial recognition images	Same as above, but once decided, John Fuller and Deputy Registrar's Rachel Madden and Erin Deveney should be involved	August 30, 2005
Within available funding, what can you accomplish?	All impacted RMV managers	August 30, 2005
Create audit system and solutions to inhibit fraud/continued mistakes – this should also serve as evaluation tool for program monitoring on an on-going basis	Cheryl Surette, Audit Manager, Paula Tosca, Director of Special Operations, Deputy Registrars Erin Deveney and Rachel Madden, Director of Branch Operations Lorraine Lague	Prior to implementation of system in branches
Determine access to system and create security levels	John Fuller, Lorraine Lague, Rachel Madden, Cheryl Surette, Registrar, Paula Tosca	Prior to implementation of system in branches
“Install” system and begin facial recognition matching	John Fuller, in cooperation with Lorraine Lague and all branch managers	Begin September 1 – end September 30, 2005

### **Evaluation**

The Director of Special Operations, in cooperation with the Directors of Audit and Branch Operations, will develop a process to audit and monitor all suspected fraudulent activity. This will include specially created reports and tracking that can be used to evaluate the results of the implementation of facial recognition technology.

A contracted person familiar with the CDL program and the facial recognition program will work in cooperation with the RMV Chief Fiscal officer and Information Technology staff to conduct interviews, gather information and write the quarterly reports to be submitted to the FMCSA.

This person will also interview involved branch managers and staff to gather relevant implementation and operations data.

The final investigative data will be analyzed to determine the outcome of investigations, which will specifically determine the usefulness, or not, of having facial recognition technology at the Registry of Motor Vehicles.

All recommendations will be in written form and distributed to all involved managers to use in senior staff decision-making efforts toward program improvement or change.

**Executive Summary/Abstract**

Herbert Osgood, Director of Driver Licensing, is the contact person whose telephone number is [REDACTED] and whose address is [REDACTED].

The RMV is seeking a portion of the funding needed in the amount of \$250,00 to acquire facial recognition technology at the RMV. It has another commitment for some funding from the Executive Office of Public Safety, but not enough to meet the costs involved.

This system has the potential to be programmed with photographs and identification information from outside entities of terrorists and other people who may be on some type of targeted arrest or warrant list. In addition, a police or other law enforcement department or agency can give the RMV an artist's rendering of a suspect to run against the database and it will find that person if they are in the files.

What makes this project enormously expensive is the option to "scrub" the existing database. In other words, to determine how many licenses already IN the database, have a duplicate or questionable match in the database. Preliminary pilot testing of 120,000 images returned 96 such "matching" images.

This was "controlled" testing, in that the RMV selected a specific demographic in choosing which images to run against the database. This had a specific "positive" result in the number of matches returned. During this pilot testing the RMV learned that another state that has been using facial recognition for more than one year now, returns about 1- 3 cases that require full investigation, after the images are reviewed for clerical errors, name changes, etc. While this is not a huge number, it only takes one person to create irreparable harm. If the RMV and the police can remove this one person from the driving population, the CDL program, the RMV in general, and the public at large are more secure.

Any system might have great potential, but it is only through effective planning and management that this full potential can be realized.

There are many issues to be faced and resolved by the agency decision-makers to ensure the success of any and all of these strategies to combat licensing fraud.

Here are just a few examples of the elements Facial Recognition Program Development must and will include:

- Deciding customization options and integration of facial recognition with existing IT systems
- Deciding whether "outside" agencies should and can have access to enrolled images
- Within available funding, deciding what can be accomplished
- Creation of an audit system and solutions to inhibit fraud and clerical mistakes

All CDL license applicants, as well as renewals and out-of-state transfers will be enrolled in facial recognition software, and their images checked against the existing database, then stored in it. Of course, any suspicious finds will be investigated.

**Budget Narrative:**

As previously described, an integral part of facial recognition is the administrative burden to investigate and examine the identified images. Therefore, any cost analysis must include the establishment and funding of that administrative, investigative unit. This unit, along with the existing Audit unit of the RMV are crucial to the development of formal evaluation of facial recognition technology and the impact it has on licensing fraud.

In addition, there are one-time set-up costs that include hardware image stations, software development and licensing.

The cost for this technology has been priced at \$1,493,275, this is an all-inclusive price, with the exception of the cost to perform a “scrub” of the database. This “scrub” would mean that images would be run against each other in the existing database, to determine where there are people with more than one image, with more than one name and demographics, whether someone is in the database with the same image and signature, but under two completely different names or license numbers.

In other words, this scrub would identify people in the database now who have multiple identities. This process will be on-going, while facial recognition is implemented for all new passenger license applicants, transfers from out of state, and renewals, as well as for all new CDL license applicants, renewals and out of state transfers. While this is a one-time cost, to perform the scrub of approximately 7 million images, it will take four years to complete the scrubbing of the entire database. This is because this process has to happen overnight, when normal licensing production is not in process.

The RMV has a commitment of partial funding from the Executive Office of Public Safety (EOPS), toward this facial recognition purchase, and is seeking \$250,000 from the FMCSA to add to that figure. The \$250,000 the RMV is seeking from FMCSA will pay for the \$100,000 “scrub,” and two investigators with a law enforcement background. It will be the job of these investigators to investigate all of the cases found when the images are run in the facial recognition software, where fraud appears to have been perpetrated. It is hoped that prosecution will result, where necessary, from these in-depth investigations.

**Special note:**

There are proprietary issues with regard to the licensing software currently in use that would make it extraordinarily difficult, time consuming and far more expensive, if the RMV were to *not* sole-source this contract to the vendor who currently provides license production services to the MA RMV



# Budget Detail Worksheet

**Purpose:** The Budget Detail Worksheet may be used as a guide to assist you in the preparation of the budget and budget narrative. You may submit the budget and budget narrative using this form or in the format of your choice (plain sheets, your own form, or a variation of this form). However, all required information (including the budget narrative) must be provided. Any category of expense not applicable to your budget may be deleted.

**A. Personnel** - List each position by title and name of employee, if available. Show the annual salary rate and the percentage of time to be devoted to the project. Compensation paid for employees engaged in grant activities must be consistent with that paid for similar work within the applicant organization.

Name/Position	Computation	Cost
Investigator, law enforcement experience/background	Comparative annual state salary 100%	\$60,000.00
Investigator, law enforcement experience/background	Comparative annual state salary 100%	\$60,000.00
Position 3		
Position 4		
Position 5		
Position 6		
SUB-TOTAL		\$120,000.00

**B. Fringe Benefits** - Fringe benefits should be based on actual known costs or an established formula. Fringe benefits are for the personnel listed in budget category (A) and only for the percentage of time devoted to the project. Fringe benefits on overtime hours are limited to FICA, Workman's Compensation, and Unemployment Compensation.

Name/Position	Computation	Cost
Investigator	25% of annual salary = fringe	\$15,000.00
Investigator		\$15,000.00
Fringe benefit 3		
Fringe benefit 4		
Fringe benefit 5		
SUB-TOTAL		\$30,000.00
Total Personnel & Fringe Benefits		\$150,000.00



**C. Travel** - Itemize travel expenses of project personnel by purpose (e.g., staff to training, field interviews, advisory group meeting, etc.). Show the basis of computation (e.g., six people to 3-day training at \$X airfare, \$X lodging, \$X subsistence). In training projects, travel and meals for trainees should be listed separately. Show the number of trainees and the unit costs involved. Identify the location of travel, if known. Indicate source of Travel Policies applied, Applicant or Federal Travel Regulations.

Purpose of Travel	Location	Item	Computation	Cost
Travel entry 1, two lines per entry				
Travel entry 2				
Travel entry 3				
Travel entry 4				
Travel entry 5				
Travel entry 6				
Travel entry 7				
<b>TOTAL</b>				\$0.00

**D. Equipment** - List non-expendable items that are to be purchased. Non-expendable equipment is tangible property having a useful life of more than two years and an acquisition cost of \$5,000 or more per unit. (Note: Organization's own capitalization policy may be used for items costing less than \$5,000). Expendable items should be included either in the "supplies" category or in the "Other" category. Applicants should analyze the cost benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technical advances. Rented or leased equipment costs should be listed in the "Contractual" category. Explain how the equipment is necessary for the success of the project. Attach a narrative describing the procurement method to be used.

Item	Computation	Cost
Equipment entry 1, one line per entry		
equipment entry 2		
equipment entry 3		
equipment entry 4		
equipment entry 5		
<b>TOTAL</b>		\$0.00

**E. Supplies** - List items by type (office supplies, postage, training materials, copying paper, and expendable equipment items costing less than \$5,000, such as books, hand held tape recorders) and show the basis for computation. (Note: Organization's own capitalization policy may be used for items costing less than \$5,000). Generally, supplies include any materials that are expendable or consumed during the course of the project.

Supply Items	Computation	Cost
Hardware desktop image stations	one-time cost \$1,600 x 4 units	\$6,400.00
Licensing for non-Digimarc (license vendor) products	one-time cost \$255. x 4	\$1,020.00
supply item 3		
supply item 4		
supply item 5		
supply item 6		
supply item 7		
supply item 8		
supply item 9		
		<b>TOTAL</b> \$7,420.00

**F. Construction** - As a rule, construction costs are not allowable. In some cases, minor repairs or renovations may be allowable. Check with the program office before budgeting funds in this category.

Purpose	Description of Work	Cost
four lines per entry, use boxes below or an additional page for more space if required		
		<b>TOTAL</b> \$0.00

**G. Consultants/Contracts** - Indicate whether applicant's formal, written Procurement Policy or the Federal Acquisition Regulations are followed.

**Consultant Fees:** For each consultant enter the name, if known, service to be provided, hourly or daily fee (8-hour day), and estimated time on the project. Consultant fees in excess of \$450 per day require additional justification and prior approval from OJP.

Name of Consultant	Service Provided	Computation	Cost
Designated Info Technology staff person	development of software to support image file transfer - one-time development costs	\$82 per hour x 1050 hrs	\$86,100.00
Supply item 1, one line per entry			
Supply item 1, one line per entry			
Supply item 1, one line per entry			
<b>Subtotal</b>			\$86,100.00

**Consultant Expenses:** List all expenses to be paid from the grant to the individual consultants in addition to their fees (i.e., travel, meals, lodging, etc.)

Item	Location	Computation	Cost
	maximum of three lines		
	maximum of three lines		
Consultant expense entry 1, one line per	maximum of three lines		
<b>Subtotal</b>			\$0.00

**Contracts:** Provide a description of the product or service to be procured by contract and an estimate of the cost. Applicants are encouraged to promote free and open competition in awarding contracts. A separate justification must be provided for sole source contracts in excess of \$100,000.

Item	Cost
Contract with Digimarc Corporation to purchase Facial Recognition software business solution to implement in RMV daily operations. This is an all-inclusive price, with the exception of \$100,000 to perform a "scrub" of the existing database	\$1,493,275.00
Contract with Digimarc, in addition to the purchase contract for facial recognition, to provide the service which would take all of the current license images (more than seven million) and attempt to determine whether or not there is a duplicate identity or fraudulent license currently in the database. This is a one-time cost. This "scrub" can only be performed at night, when license production is not on-going, and therefore, will take four years to complete.	\$100,000.00
<b>Subtotal</b>	\$1,593,275.0
<b>TOTAL</b>	\$1,679,375.0

**H. Other Costs** - List items (e.g., rent, reproduction, telephone, janitorial or security services, and investigative or confidential funds) by major type and the basis of the computation. For example, provide the square footage and the cost per square foot for rent, or provide a monthly rental cost and how many months to rent.

Description	Computation	Cost
four lines per entry, use boxes below or an additional page for more space if required		
<b>TOTAL</b>		\$0.00

**I. Indirect Costs** - Indirect costs are allowed only if the applicant has a Federally approved indirect cost rate. A copy of the rate approval, (a fully executed, negotiated agreement), must be attached. If the applicant does not have an approved rate, one can be requested by contacting the applicant's cognizant Federal agency, which will review all documentation and approve a rate for the applicant organization, or if the applicant's accounting system permits, costs may be allocated in the direct costs categories.

Description	Computation	Cost
one line per entry		\$0.00
one line per entry		
<b>TOTAL</b>		\$0.00

**Budget Summary**- When you have completed the budget worksheet, transfer the totals for each category to the spaces below. Compute the total direct costs and the total project costs. Indicate the amount of Federal requested and the amount of non-Federal funds that will support the project.

<b>Budget Category</b>		<b>Amount</b>
<b>A. Personnel</b>		<u>\$120,000.00</u>
<b>B. Fringe Benefits</b>		<u>\$30,000.00</u>
<b>C. Travel</b>		<u>\$0.00</u>
<b>D. Equipment</b>		<u>\$0.00</u>
<b>E. Supplies</b>		<u>\$7,420.00</u>
<b>F. Construction</b>		<u>\$0.00</u>
<b>G. Consultants/Contracts</b>		<u>\$1,679,375.00</u>
<b>H. Other</b>		<u>\$0.00</u>
<b>Total Direct Costs</b>		<u>\$1,836,795.00</u>
<b>I. Indirect Costs</b>		<u>\$0.00</u>
<b>TOTAL PROJECT COSTS</b>		<u>\$1,836,795.00</u>
<b>Federal Request</b>		<u>\$250,000.00</u>
<b>Non-Federal Amount</b>		<u>\$1,586,795.00</u>



Deval L. Patrick, Governor  
Richard A. Davey, Secretary & CEO  
Rachel Kaprielian, Registrar



## REQUEST FOR DIGITIZED IMAGE PRINTOUT

### DRIVER LICENSE/ ID INFORMATION (OF THE PERSON WHOSE IMAGE IS BEING REQUESTED)

NAME: \_\_\_\_\_ LICENSE ID # \_\_\_\_\_

ADDRESS: \_\_\_\_\_

### REQUESTOR INFORMATION

REQUESTOR'S NAME \_\_\_\_\_

SIGNATURE: \_\_\_\_\_ DATE: \_\_\_\_\_

CORI APPROVED AGENCY: \_\_\_\_\_

ADDRESS: \_\_\_\_\_

TELEPHONE #: \_\_\_\_\_ FAX #: \_\_\_\_\_

### REQUEST REASON ( THIS SECTION MUST BE COMPLETED WITH AN OFFICIAL BUSINESS REQUEST )

UPON COMPLETION OF INVESTIGATION, PLEASE RETURN LICENSE / ID TO THE RMV

### Request details

What type of image do you need ?

What date do you need the image by ?

☐ Color

☐ Black & White

☐ Both

Attention: Cori requests may be sent anytime, but RMV personnel are only available to process requests from 8:45 a.m. to 4:30 p.m. Monday thru Friday. If there is an emergency reason for more expeditious handling, please indicate this reason in the line below.

### RMV Contact Information ( office use only )

Cori Fax : 857-368-0649

Cori Information: 857-368-9500

☐ Picked Up

☐ Faxed

☐ Mailed

☐ Image Not on File

Date Completed: \_\_\_\_\_

Processed By :  
ACLU 14-164 Page 33

# **EXHIBIT 2**





THE COMMONWEALTH OF MASSACHUSETTS  
EXECUTIVE OFFICE OF TRANSPORTATION  
REGISTRY OF MOTOR VEHICLES

**EOT**

MITT ROMNEY  
GOVERNOR

KERRY HEALEY  
LIEUTENANT GOVERNOR

JOHN COGLIANO  
SECRETARY

ANNE L. COLLINS  
REGISTRAR

TO: Massachusetts Law Enforcement Personnel  
FROM: Anne L. Collins, Registrar  
DATE: October 31, 2006  
RE: Facial Recognition Assistance at RMV

I am writing with good news. The RMV, with the help of Massachusetts State Police, has implemented an amazing Facial Recognition System that allows a digital image – such as a license photo – to be compared against the 9.5 million images in the RMV database to identify potential “matches.” State Police and RMV staff have been using this tool since May 2006 and have successfully identified many individuals who have fraudulently applied for multiple licenses or IDs.

The newest improvement to the Facial Recognition System may help your law enforcement team. We are now able to accept digital images – such as digital mug shots – by email and compare them against the photos in the RMV database. For example, State Police recently used this tool to assist a medical examiner who was trying to identify a “John Doe.”

If you would like an image run through the Facial Recognition System, please **email** a request to [RMV-DL-FacialRecES@MassMail.State.MA.US](mailto:RMV-DL-FacialRecES@MassMail.State.MA.US). All requests should include:

- the name of your law enforcement department,
- the name of a contact person, and
- a call-back number.

Only requests received from official law enforcement email addresses can be accepted. (No personal emails will be answered.) Although the Facial Recognition Team may be reached by phone at 617-973-8952, we ask that you call only in emergencies.

When the Facial Recognition Team has run your subject and reviewed the potential matches, they will contact you by telephone. As appropriate, they will direct you to the CJIS Web so you can see the image of the subject or compare multiple images. If you are still uncertain about the results, you may come to the Facial Recognition office at the State Transportation Building, 10 Park Plaza, Boston, MA to compare hard copies of the matches. You may also prefer to have the hard copies for court purposes. Due to privacy issues, however, we are unable to send the results over the internet.

I look forward to the successes that will arise out of this collaboration and I assure you the Facial Recognition Team will do our best to assist you.

Although it appears the Facial Recognition System is “looking” at the photos, it actually converts each face into a map of thousands of data points, then compares those points. For example, it maps each subject’s eyes and measures the distance between the pupils, then searches for other images with the same distance. The System does not compare some factors that might otherwise distinguish one person from another, such as height, age, or ethnicity. Therefore, the better the quality of the image you can send, the better the potential matches will be.

**The following guidelines should be used when sending images to be run through the system.**

Facial Recognition Email Address: [RMV-DL-FacialRecES@MassMail.State.MA.US](mailto:RMV-DL-FacialRecES@MassMail.State.MA.US)

#### Ideal Image Parameters

1. Maximum Size
  - a. 1024 by 1024 pixels
  - b. 2 megabytesNote: Image properties in MSPAINT can be used to display actual image size.
2. Type
  - a. JPEG minimum compression (to fit 2 MB)
  - b. BMP
3. Cropping/ Zoom
  - a. Head compromises approximately 80% of image height (small bit of shoulders)
  - b. Head comprises 70% of width
4. Direction
  - a. Subject should be facing directly into camera
  - b. Slightly left or right is acceptable (maximum 10 degrees)
  - c. Never from below
5. Lighting
  - a. Lighting should be as bright as possible
  - b. Avoid dark shadows near the bottom of the face
6. Originals vs. Copies
  - a. The original image should be submitted for optimum results.
  - b. Every time the image is copied it is changed slightly
  - c. The investigating officer should only use Photo Shop or similar software on the original image if an adjustment is required.
7. Eyeglasses
  - a. If images are available with and without glasses, both should be sent.

# **EXHIBIT 3**



## Department of State Police Superintendent's Memo

Effective Date <b>February 21, 2008</b>	Number <b>08-SM-07</b>
Subject <b>Revised Access to Facial Recognition System</b>	

The Registry of Motor Vehicles has revised the e-mail address that Law Enforcement Agencies may utilize to send requests to have an image run through the Facial Recognition System. The e-mail address is:

MSP-DL-FacialRecES@MassMail.State.MA.US

Requests shall include name, rank, ID #, current station or duty assignment and a call back number. As before, only requests received from official, department assigned e-mail addresses will be accepted. (Requests being made via personal e-mail accounts will not be accepted or answered.)

After the Facial Recognition Team has determined if there is a hit on the subject, the sender will be contacted by telephone with the results. The sender will then be directed to CJIS Web so the image of the subject can be viewed or compared with multiple images. If the sender is still uncertain regarding the results, they may come to the Facial Recognition office at the State Transportation Building: 10 Park Plaza, 2<sup>nd</sup> Floor, Boston, MA to compare the hard copies of the images. For court purposes, it may be preferable to have the hard copies. Due to privacy issues, requests to send the results over the internet will not be accepted.

The existing ideal image parameters should be followed when sending images to be run through the system:

- Maximum Size:
  - a. 1024 by 1024 pixels
  - b. 2 megabytesNote: Image properties in MSPAINT can be used to display actual image size.
- Type:
  - a. JPEG minimum compression (to fit 2 MB)
  - b. BMP
- Cropping/ Zoom:
  - a. Head comprises approximately 80% of image height (small bit of shoulders)
  - b. Head comprises 70% of width

- Subject should be facing directly into camera:
  - a. Slightly left or right is acceptable (maximum 10 degrees)
  - b. Never from below
- Lighting should be as bright as possible:
  - a. Avoid dark shadows near the bottom of the face
- The original image should be submitted for optimum results:
  - a. Every time the image is copied it is changed slightly
  - b. The investigating officer should only use Photo Shop or similar software on the original image if an adjustment is required.
- If images are available with and without glasses, both should be sent.

All inquiries must be related to an ongoing criminal investigation. In addition, officers may want to utilize SP 627, the Facial Recognition Request Form as part of their investigation. In cases of emergencies only officers may call the Facial Recognition Team directly at 617-973-8952.

**OFFICIAL:**

**Mark F. Delaney**  
**Colonel / Superintendent**



# Facial Recognition Request Form

**Directions:**

- 1) Fill out all information as completely as possible.
- 2) Fax completed form to the MVRS-Facial Recognition Team at 617-973-8982.

Date: \_\_\_\_\_ Case #: \_\_\_\_\_

Requesting Agency: \_\_\_\_\_

Requestors Name: \_\_\_\_\_

ID #: \_\_\_\_\_ Phone #: \_\_\_\_\_ Fax #: \_\_\_\_\_

Official E-mail Address: \_\_\_\_\_

---

**Probe Information:**

License #: \_\_\_\_\_ SS #: \_\_\_\_\_

Last Name: \_\_\_\_\_ First Name: \_\_\_\_\_

Notes: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

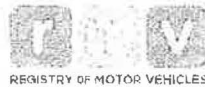
\_\_\_\_\_

**Contact the Facial Recognition Team at 617-973-8952 upon completion of case for license(s) revocation, flagging, and activity hold placement on record(s).**

**For MVRS-Facial Recognition Team Use Only:**

Date of search: _____	Performed by: _____
<input type="checkbox"/> Record Flagged	<input type="checkbox"/> Record Released
<input type="checkbox"/> FR Notes added	

# **EXHIBIT 4**



## AGREEMENT FOR ACCESS TO RECORDS AND DATA MAINTAINED BY THE REGISTRY OF MOTOR VEHICLES

This agreement (hereinafter "Agreement") is made and entered into by and between the Massachusetts Department of Transportation, through its Registry of Motor Vehicles Division (hereinafter the "RMV"), a body politic and corporate, and public instrumentality of the Commonwealth, established and operating pursuant to M.G.L. c. 6C and Brookline Police Department

its affiliates and/or subsidiaries or, (hereinafter the "REQUESTOR"). The Terms and Conditions of this Agreement shall be binding upon either party's legal successor.

### RECITALS

WHEREAS, the RMV stores personal and confidential information protected by the federal Driver Privacy Protection Act (18 U.S.C. § 2721 et seq.) (hereinafter "DPPA") in its database and

WHEREAS, the RMV is authorized under the DPPA to provide and/or allow access to records and data in its database containing personal and confidential information to permitted users for permissible purposes, as defined under the DPPA and

WHEREAS, the RMV has established a Database to maintain and provide access to such records and data and

WHEREAS, state and federal law, including the DPPA, protect personal information maintained in the records of the RMV and

WHEREAS, Requestor desires to obtain records and data which may contain personal information from the RMV and

WHEREAS, Requestor agrees that it is a permitted user of RMV records and data under the DPPA and

WHEREAS, the RMV requires that Requestor execute this written Agreement to ensure that records and data obtained from the RMV will be used only for permissible purposes, as set forth in the DPPA, and that personal information contained in said records will be safeguarded and protected before Requestor obtains access to said records and data;

NOW THEREFORE, in consideration of the foregoing recitals (which are hereby incorporated into and made an integral part of this Agreement), as well as the duties and obligations set forth in this Agreement, it is agreed by and between the parties as follows:



### TERMS AND CONDITIONS

1. **Permitted Use:** Requestor hereby certifies that Requestor is permitted to obtain access to RMV data under the provisions of the DPPA as it is: **PICK FROM BELOW (CHECK ALL THAT APPLY):**

- ☐ A. An insurance company licensed by the Massachusetts Division of Insurance to write private passenger automobile policies in Massachusetts or an authorized agent or service carrier wherein the records and data will be used to the extent authorized in the safe driver insurance plan and for the purpose of complying with the requirements of M.G.L. Chapter 90, §§1A, 34A, 34B and 34H pertaining to motor vehicle liability policies;
- ☐ B. An insurer or insurance support organization, a self-insured entity or an agent, employee or contractor of such, wherein the records and data will be used in connection with claims investigation activities, anti-fraud activities, rating or underwriting;
- ☒ C. A federal, state or local governmental agency wherein the records and data will be used for a permitted use as solely determined by the RMV and to carry out the official functions of such agency;
- ☐ D. A legitimate business, which in the normal course of business will use RMV data solely for the purpose of verifying the accuracy of personal information submitted by an individual to the Requestor's, agents, contractors or employees;
- ☐ E. A private entity or individual acting on behalf of a federal, state or local governmental agency for item C above wherein the RMV's records and data are used to carry out the official functions of such federal, state, or local governmental agency;
- ☐ F. An authorized lender or lien holder that participates in the RMV's Electronic Lien Holder Program which permits electronic communication of certain title and lien information, for the purpose of obtaining information about, posting and releasing motor vehicle liens;
- ☐ G. A licensed motor vehicle dealership or insurance agency or other permitted entity that has been approved by the RMV to participate in its EVR program and to register motor vehicles electronically
- ☐ H. A Driving School licensed by the RMV under M.G.L. chapter 90, sections 32G and 32G1/2;
- ☐ I. A private entity that the RMV engages to provide programs in driver attitudinal training, or similar services
- ☐ J. A private entity acting on the behalf of any of those listed in items A through I.

2. **Access To and Use of Personal Data:** Requestor certifies it will use RMV data solely for purposes consistent with Paragraph 1 of this Agreement. Furthermore, the Requestor shall not use any personal information obtained pursuant to this Agreement for any purpose that is not permitted under Massachusetts or Federal laws, rules or regulations; as may be amended from time to time and the Requestor agrees it will comply with all applicable laws and regulations respecting access to and use of personal information, including the Federal Driver Privacy Protection Act (the "DPPA") (18 U.S.C. §2721 et seq.), the Massachusetts Identity Theft Act, G.L. c. 93H, the Standards for the Protection of Personal Information of Residents of the Commonwealth 201 C.M.R. 17.00 and Executive Order 504. The Requestor represents that it has read the DPPA, M.G.L. c. 93H, the Standards for the Protection of Personal Information of Residents of the Commonwealth 201 C.M.R. 17.00 and Executive Order 504 and will comply with such laws and Order and all other applicable laws, state or federal, regarding access to and the use of motor vehicle records, personal information and data privacy and protection, as such laws may be amended from time to time. The Requestor further agrees that Personal Information accessed under this Agreement shall not be used to create or aggregate the data for any purpose, except as specifically provided by federal or state law or other sections of this Agreement.
3. **Method of Access:** Requestor will access data provided by the RMV via one or more of the following methods of access :
  - a. Obtain files from and/or exchange files with the RMV using Secure File Transfer Protocol ("SFTP").
  - b. Call RMV Web Services;
  - c. Utilize the eServices Portal or Business Portal;
4. **Training and Policy Acknowledgement:**
  - a. Requestor agrees to participate in and complete any training programs in the use of the RMV database, as the RMV in its sole discretion, deems necessary.
  - b. Requestor agrees to ensure that its employees accessing RMV data complete any and all RMV policy acknowledgement forms.
5. **Data:** The RMV may, at its sole discretion and based on the Permitted Use(s) defined in Paragraph 1 above, make its records and data available to Requestor solely to perform the business functions as defined in the Permitted Use in paragraph 1.
6. **Term:** This Agreement shall be in effect for three years, and may be renewed for additional three year periods upon notification from the RMV. The RMV will notify the Requestor on two separate occasions in the 30 day period prior to the expiration of the Agreement via the Requestor's e-mail address, as provided. If the Requestor does not renew the Agreement prior to its expiration date, all access will terminate on that date.
7. **Cost:** The requestor will pay the RMV any and all applicable fees established in 801 CMR 4.02, which may be subject to change.
8. **Electronic Security Requirements:**
  - a. The Requestor, by this agreement, certifies it has an information security program in place that follow current industry design and best practices, including, but not limited to those published by The National Institute of Standards & Technology (NIST), the SANS

(SysAdmin, Audit, Network, Security (SANS) Institute), and other recognized bodies to prevent unauthorized electronic access to RMV data or to its database.

- b. For All Requestors , using any Access Method, Requestor agrees to do the following:
  - i. Have written procedures in place to insure the electronic safety, physical security and confidentiality of RMV data in accordance with paragraph 10 of this Agreement;
  - ii. Have written procedures in place that insure RMV data is accessed only for permitted uses under the DPPA and consistent with paragraph 10 of this Agreement.
- c. For Requestors Who Select Web Services or SFTP Option Under Paragraph 3, Requestor agrees to do the following:
  - i. Assign a unique ID to each end user who will access RMV data.
  - ii. Implement written password policies and procedures that follow current industry design and best practices such as:
    - a. those published by The National Institute of Standards & Technology (currently SP800-63b section 5);
    - b. the SANS (SysAdmin, Audit, Network, Security Institute) Password Construction Guidelines (currently SANS document section 4) and
    - c. those published by other recognized bodies such as IRS1075 (currently section 9.3.7.5).
  - iii. The standards referenced in subsection ii above must be designed to prevent unauthorized access to RMV data or to its database.
  - iv. Deactivate the unique ID immediately when the end user leaves the Requestor's employment or when the ID has not been used for a period of 90 days.
  - v. Maintain an electronic log of all transactions with the RMV for 5 years. The log shall contain all the transactions performed by each end user including the end user's unique ID (if applicable), the end-user's full name, date and time of each transaction performed and/or inquiry.
  - vi. Respond within 3 business days to the RMV's request to review a specific transaction or series of transactions including the end user's name, unique ID, dates, times and reason for the transaction(s). The RMV may, but is not required, to inform the Requestor as to its reason for the request.
  - vii. Failure to comply with subsections i-vi above may result in termination of the Agreement under the provisions of paragraph 12.

9. **A. Data Retention/Audit For SFTP And Web Services Users:** The SFTP and/or Web Services Requestor shall at all times adhere to the data retention and destruction requirements of M.G.L. Chapter 93I and the Massachusetts Public Records Law. Any data obtained from the RMV shall be shredded, destroyed or disposed of in compliance with Chapter 93I after its business purpose has expired. The Requestor shall maintain a record of transactions it performs using RMV data for a period of 5 years. Such record shall include the name of the person or entity that accessed the data; the time and date the data was provided to said person or entity and the customer information. The RMV may in its discretion audit all such documentation. The RMV will provide

the Requestor with written notice at least three (3) business days prior to said audit, which shall be performed with the reasonable cooperation of the Requestor. In the event the Requestor cannot provide a legitimate reason for accessing said data, said failure to do so may constitute a material breach under paragraph 12 of this Agreement. Furthermore, if the RMV's audit reveals inaccuracies or a violation of any provision of this Agreement, said violation or inaccuracies may be considered a material breach under paragraph 12 of the Agreement. If the Requestor does not have an office location in Massachusetts, upon request, the Requestor will forward all records to the RMV at the time and place designated by the RMV.

**B. Data Retention/Audit For eServices Portal or Business Portal Requestors:** The eServices Portal and Business Portal Requestor shall at all times adhere to the data retention and destruction requirements of M.G.L. Chapter 93I and the Massachusetts Public Records Law. Any data obtained from the RMV shall be shredded, destroyed or disposed of in compliance with Chapter 93I after its business purpose has expired. The RMV may track and audit all business transactions. The RMV may in its sole discretion require the requestor to explain and/or demonstrate its legitimate business purpose or permitted use for accessing the RMV's data for any particular transaction. Failure by the Requestor to do so may constitute a material breach under paragraph 12 of this Agreement. If the Requestor does not have an office location in Massachusetts, upon request the Requestor will forward all records to the RMV at the time and place designated by the RMV.

10. **Physical Security Of Data and Confidentiality:** The Requestor shall do the following:
- Ensure that RMV records are not visible to unauthorized individuals;
  - Shred or deposit RMV records into a locked shredder container when no longer needed;
  - Never knowingly obtain, disclose or use RMV records for a purpose not permitted under the DPPA. Requestor may be liable for impermissible dissemination of personal information to any individual to whom the personal information pertains;
  - Never misrepresent Requestor's identity or make a false statement in connection with a request for personal information with the intention of obtaining said information in a manner not authorized under this Agreement or the DPPA;
  - Never disseminate RMV records unless such dissemination is required by the Requestor's job duties;
  - Never use RMV records in the furtherance of an illegal act, including a violation of any criminal or civil laws;

11. **A. Background Checks For Requestors Who Receive Personal Information Contained in RMV Records and Data:**
- For Requestors Who Select SFTP, Web Services & eServices Option Under Paragraph 3: Prior to permitting access to the RMV's records and data, Requestor shall ensure through background checks that its employees, contractors and agents who have access to or who may view RMV data have not been convicted of a felony involving violence, dishonesty, deceit or indecency. A Requestor's employee, contractor or agent who has been convicted of such a felony shall not be qualified to access RMV data or view its data. For eServices Portal Administrators a background check will be conducted by the RMV.

- b. For Requestors Who Select the Business Portal Option under Paragraph 3: The RMV shall conduct background checks to ensure that the proposed employee, contractor and agent who will have access to or who may view RMV data has not been convicted of a felony involving violence, dishonesty, deceit or indecency. A Requestor's employee, contractor or agent who has been convicted of such a felony shall not be authorized to access the RMV database or view its data.

12. **Termination for Breach:** In addition to any termination of rights contained in this Agreement herein, the RMV may immediately terminate the Agreement and the Requestor's access to RMV data at any time, if the RMV determines in the exercise of its sole discretion, that the Requestor engaged in a material violation of any term of this Agreement, the DPPA, M.G.L. c. 93H, Executive Order 504, or any other law pertaining to the privacy of motor vehicle records. The RMV shall have no liability to the Requestor for terminating the Agreement under this provision.
13. **Right to Appeal:** The Requestor shall have the right to appeal the RMV's decision to terminate Requestor's access to RMV data pursuant to paragraph 12 above. Appeals should be made in writing and should be addressed to the Registrar of Motor Vehicles ("Registrar"). If no such appeal is made within 30 days of the termination, the termination shall be final. If the Requestor files an appeal within said 30 days period, the Registrar shall review the RMV's decision to terminate and shall make a final determination as to whether the terms of this Agreement were breached and, if so, whether the termination of access was appropriate. In making the final determination, the Registrar may consider any documentation proffered by the Requestor evidencing affirmative steps taken to prevent similar violations of this Agreement. The Registrar's decision is final and dispositive and no further appeal process is available.
14. **30 Day Termination:** Notwithstanding paragraph 5, this Agreement may be terminated by either party at any time upon thirty (30) days written notice. This agreement may be immediately terminated without advance notification upon any material breach of any covenant by either party, or if the performance of this Agreement by the RMV is made impossible or impractical, as determined in the sole reasonable judgment of the RMV, or if the requestor has not accessed the RMV's data base for a period of ninety(90) days, by any order of any Court, or any action of the Legislature of the Commonwealth of Massachusetts. Notice of termination shall be in writing signed by a duly-authorized representative of the terminating party and deposited with the United States Postal Service correctly addressed and postage prepaid.
15. **Indemnification:** The Requestor agrees to defend, hold harmless and indemnify the RMV, the Massachusetts Department of Transportation, the Commonwealth of Massachusetts and their employees and agents from any and all claims, actions, damages, or losses which may be brought or alleged against them for the negligent, improper, or unauthorized access, use or dissemination of the personal information contained in the RMV data. The Requestor shall indemnify and hold harmless the Commonwealth of Massachusetts and the Massachusetts Department of Transportation, and the RMV against any liability, claim loss, damage or expense, of every nature and kind in law or equity, arising out of or in connection with any misuse or misappropriation of any RMV Data obtained from the RMV; any failure of the Requestor to comply with any applicable provisions of State or Federal laws or regulations regarding privacy of motor vehicle records or data; any failure to safeguard and limit access to the RMV Data as



- required herein; and/or any other acts or omissions of the Requestor or its employees or agents in connection with the performance, exercise, or enjoyment of this Agreement, including without limitation reasonable attorney's fees and other costs of defending any such claim or action. The obligations under this paragraph shall survive the termination of this Agreement.
16. **Non-Assignment:** The Requestor shall not assign or in any way transfer any interest in this Agreement.
  17. **Non-Exclusivity:** The Requestor acknowledges that this Agreement is not an exclusive agreement. At its sole discretion the RMV may enter into agreements with other parties for the same or similar services as provided by this Agreement, on such terms and conditions as the RMV determines in its sole discretion.
  18. **Warranty:** The RMV makes no representation or warranty, express or implied, with respect to the accuracy of any RMV Data from a source other than the RMV. Therefore, except for acts or omissions that constitute gross negligence or willful misconduct by the Commonwealth of Massachusetts, the Massachusetts Department of Transportation, the RMV, their employees or agents, neither the Commonwealth of Massachusetts, the Massachusetts Department of Transportation, the RMV, or their employees or agents shall be liable to the Requestor for any costs, claims, liability, damages, expenses, lost production, or any other loss of any nature or kind, in law or equity, in connection with this Agreement, including but not limited to inaccurate, incomplete or unavailable RMV data.
  19. **Litigation Notice:** The Requestor shall immediately notify the Office of the General Counsel at the Massachusetts Department of Transportation in the event that it is sued or litigation is filed concerning the Requestor's use of RMV data.
  20. **Notice of Data Breach:** The Requestor shall immediately notify the Chief Information Security Office for the Massachusetts Department of Transportation at [InfoSecTeam@dot.state.ma.us](mailto:InfoSecTeam@dot.state.ma.us) in the event of a data breach or misuse of RMV data. The Requestor is responsible for all notifications and remediation pursuant to M.G.L. Chapter 93H.
  21. **Forum:** This agreement shall be construed under and governed by the laws and Executive Order 504 of the Commonwealth of Massachusetts.
  22. **Discrimination:** The Requestor shall not engage in any unlawful discrimination against any person based upon the RMV Data obtained pursuant to this Agreement, and the requestor agrees to comply with all applicable State and Federal laws, rules and regulations prohibiting discrimination in employment, including but not limit to 42 USC 12101, 28 CFR Part 35, 29 USC 791 et seq., Massachusetts General Laws Chapter 151 B and Chapter 272, §92A and §98 et seq. and Executive Orders 227, 237, and 246, or any amendments to such provisions.
  23. **Severability Clause:** In the event that any provision in this agreement shall be or become invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby and such provision shall be ineffective only to the extent of such invalidity, illegality or unenforceability.
  24. **Complete Instrument:** This Agreement constitutes the entire agreement of the parties and supersedes all other prior written or oral agreements between the parties with respect to subject matter hereof. This Agreement may be changed, modified or amended at any time only by an instrument in writing, signed by duly authorized representatives of both parties hereto.

25. **Notice:** Notice required or permitted by this Agreement shall be addressed to the address(s) as maintained by the requestor on their company profile on the RMV Web eServices or Business Portal or as follows:

To the RMV:

BY MAIL: MassDOT Registry of Motor Vehicles Division  
RMV IS Security  
25 Newport Avenue Extension  
Quincy, MA 02172  
BY E-MAIL: RMVBUSINESSPARTNERS@state.ma.us

To NAME:

BY MAIL: Brookline Police Department  
350 Washington Street  
Brookline, MA 02445-6800  
BY E-MAIL: swilder@brooklinema.gov

Any party may change its address for the purposes of receipt of notices by providing written notice to the other party in accordance with this paragraph.

26. **Execution:** This Agreement may be executed in one or more counterparts, each of which will be deemed to be an original copy of this Agreement and all of which, when taken together, will be deemed to constitute one and the same agreement. The facsimile, email or other electronically delivered signatures of the parties shall be deemed to constitute original signatures, and facsimile or electronic copies hereof shall be deemed to constitute duplicate originals

IN WITNESS WHEREOF, the parties have hereto caused this instrument to be executed by their duly authorized officials or officers.

The Massachusetts Department  
Of Transportation, Registry of Motor  
Vehicles Division

NAME: Brookline Police Department

BY: [Signature]  
TITLE: Registrar

BY: [Signature]

TITLE: Director of Technology

DATE: 2.2.18

DATE: 03/03/2018







REGISTRY OF MOTOR VEHICLES



## AGREEMENT FOR ACCESS TO RECORDS AND DATA MAINTAINED BY THE REGISTRY OF MOTOR VEHICLES

This agreement (hereinafter "Agreement") is made and entered into by and between the Massachusetts Department of Transportation, through its Registry of Motor Vehicles Division (hereinafter the "RMV"), a body politic and corporate, and public instrumentality of the Commonwealth, established and operating pursuant to M.G.L. c. 6C and FBI Boston

its affiliates and/or subsidiaries or, (hereinafter the "REQUESTOR"). The Terms and Conditions of this Agreement shall be binding upon either party's legal successor.

### RECITALS

WHEREAS, the RMV stores personal and confidential information protected by the federal Driver Privacy Protection Act (18 U.S.C. § 2721 et seq.) (hereinafter "DPPA") in its database and

WHEREAS, the RMV is authorized under the DPPA to provide and/or allow access to records and data in its database containing personal and confidential information to permitted users for permissible purposes, as defined under the DPPA and

WHEREAS, the RMV has established a Database to maintain and provide access to such records and data and

WHEREAS, state and federal law, including the DPPA, protect personal information maintained in the records of the RMV and

WHEREAS, Requestor desires to obtain records and data which may contain personal information from the RMV and

WHEREAS, Requestor agrees that it is a permitted user of RMV records and data under the DPPA and

WHEREAS, the RMV requires that Requestor execute this written Agreement to ensure that records and data obtained from the RMV will be used only for permissible purposes, as set forth in the DPPA, and that personal information contained in said records will be safeguarded and protected before Requestor obtains access to said records and data;

NOW THEREFORE, in consideration of the foregoing recitals (which are hereby incorporated into and made an integral part of this Agreement), as well as the duties and obligations set forth in this Agreement, it is agreed by and between the parties as follows:

### TERMS AND CONDITIONS

1. **Permitted Use:** Requestor hereby certifies that Requestor is permitted to obtain access to RMV data under the provisions of the DPPA as it is: **PICK FROM BELOW (CHECK ALL THAT APPLY):**

- ☐ A. An insurance company licensed by the Massachusetts Division of Insurance to write private passenger automobile policies in Massachusetts or an authorized agent or service carrier wherein the records and data will be used to the extent authorized in the safe driver insurance plan and for the purpose of complying with the requirements of M.G.L. Chapter 90, §51A, 34A, 34B and 34H pertaining to motor vehicle liability policies;
- ☐ B. An insurer or insurance support organization, a self-insured entity or an agent, employee or contractor of such, wherein the records and data will be used in connection with claims investigation activities, anti-fraud activities, rating or underwriting;
- ☒ C. A federal, state or local governmental agency wherein the records and data will be used for a permitted use as solely determined by the RMV and to carry out the official functions of such agency;
- ☐ D. A legitimate business, which in the normal course of business will use RMV data solely for the purpose of verifying the accuracy of personal information submitted by an individual to the Requestor's, agents, contractors or employees;
- ☐ E. A private entity or individual acting on behalf of a federal, state or local governmental agency for item C above wherein the RMV's records and data are used to carry out the official functions of such federal, state, or local governmental agency;
- ☐ F. An authorized lender or lien holder that participates in the RMV's Electronic Lien Holder Program which permits electronic communication of certain title and lien information, for the purpose of obtaining information about, posting and releasing motor vehicle liens;
- ☐ G. A licensed motor vehicle dealership or insurance agency or other permitted entity that has been approved by the RMV to participate in its EVR program and to register motor vehicles electronically;
- ☐ H. A Driving School licensed by the RMV under M.G.L. chapter 90, sections 32G and 32G1/2;
- ☐ I. A private entity that the RMV engages to provide programs in driver attitudinal training, or similar services;
- ☐ J. A private entity acting on the behalf of any of those listed in items A through I.

2. **Access To and Use of Personal Data:** Requestor certifies it will use RMV data solely for purposes consistent with Paragraph 1 of this Agreement. Furthermore, the Requestor shall not use any personal information obtained pursuant to this Agreement for any purpose that is not permitted under Massachusetts or Federal laws, rules or regulations, as may be amended from time to time and the Requestor agrees it will comply with all applicable laws and regulations respecting access to and use of personal information, including the Federal Driver Privacy Protection Act (the "DPPA") (18 U.S.C. §2721 et seq.), the Massachusetts Identity Theft Act, G.L. c. 93H, the Standards for the Protection of Personal Information of Residents of the Commonwealth 201 C.M.R. 17.00 and Executive Order 504. The Requestor represents that it has read the DPPA, M.G.L. c. 93H, the Standards for the Protection of Personal Information of Residents of the Commonwealth 201 C.M.R. 17.00 and Executive Order 504 and will comply with such laws and Order and all other applicable laws, state or federal, regarding access to and the use of motor vehicle records, personal information and data privacy and protection, as such laws may be amended from time to time. The Requestor further agrees that Personal Information accessed under this Agreement shall not be used to create or aggregate the data for any purpose, except as specifically provided by federal or state law or other sections of this Agreement.
3. **Method of Access:** Requestor will access data provided by the RMV via one or more of the following methods of access :
  - a. Obtain files from and/or exchange files with the RMV using Secure File Transfer Protocol ("SFTP").
  - b. Call RMV Web Services;
  - c. Utilize the eServices Portal or Business Portal;
4. **Training and Policy Acknowledgement:**
  - a. Requestor agrees to participate in and complete any training programs in the use of the RMV database, as the RMV in its sole discretion, deems necessary.
  - b. Requestor agrees to ensure that its employees accessing RMV data complete any and all RMV policy acknowledgement forms.
5. **Data:** The RMV may, at its sole discretion and based on the Permitted Use(s) defined in Paragraph 1 above, make its records and data available to Requestor solely to perform the business functions as defined in the Permitted Use in paragraph 1.
6. **Term:** This Agreement shall be in effect for three years, and may be renewed for additional three year periods upon notification from the RMV. The RMV will notify the Requestor on two separate occasions in the 30 day period prior to the expiration of the Agreement via the Requestor's e-mail address, as provided. If the Requestor does not renew the Agreement prior to its expiration date, all access will terminate on that date.
7. **Cost:** The requestor will pay the RMV any and all applicable fees established in 801 CMR 4.02, which may be subject to change.
8. **Electronic Security Requirements:**
  - a. The Requestor, by this agreement, certifies it has an information security program in place that follow current industry design and best practices, including, but not limited to those published by The National Institute of Standards & Technology (NIST), the SANS

(SysAdmin, Audit, Network, Security (SANS) Institute), and other recognized bodies to prevent unauthorized electronic access to RMV data or to its database.

- b. For All Requestors, using any Access Method, Requestor agrees to do the following:
  - i. Have written procedures in place to insure the electronic safety, physical security and confidentiality of RMV data in accordance with paragraph 10 of this Agreement;
  - ii. Have written procedures in place that insure RMV data is accessed only for permitted uses under the DPPA and consistent with paragraph 10 of this Agreement.
- c. For Requestors Who Select Web Services or SFTP Option Under Paragraph 3. Requestor agrees to do the following:
  - i. Assign a unique ID to each end user who will access RMV data.
  - ii. Implement written password policies and procedures that follow current industry design and best practices such as:
    - a. those published by The National Institute of Standards & Technology (currently SP800-63b section 5);
    - b. the SANS (SysAdmin, Audit, Network, Security Institute) Password Construction Guidelines (currently SANS document section 4) and
    - c. those published by other recognized bodies such as IRS1075 (currently section 9.3.7.5).
  - iii. The standards referenced in subsection ii above must be designed to prevent unauthorized access to RMV data or to its database.
  - iv. Deactivate the unique ID immediately when the end user leaves the Requestor's employment or when the ID has not been used for a period of 90 days.
  - v. Maintain an electronic log of all transactions with the RMV for 5 years. The log shall contain all the transactions performed by each end user including the end user's unique ID (if applicable), the end-user's full name, date and time of each transaction performed and/or inquiry.
  - vi. Respond within 3 business days to the RMV's request to review a specific transaction or series of transactions including the end user's name, unique ID, dates, times and reason for the transaction(s). The RMV may, but is not required, to inform the Requestor as to its reason for the request.
  - vii. Failure to comply with subsections i-vi above may result in termination of the Agreement under the provisions of paragraph 12.

9. **A. Data Retention/Audit For SFTP And Web Services Users:** The SFTP and/or Web Services Requestor shall at all times adhere to the data retention and destruction requirements of M.G.L. Chapter 93J and the Massachusetts Public Records Law. Any data obtained from the RMV shall be shredded, destroyed or disposed of in compliance with Chapter 93J after its business purpose has expired. The Requestor shall maintain a record of transactions it performs using RMV data for a period of 5 years. Such record shall include the name of the person or entity that accessed the data; the time and date the data was provided to said person or entity and the customer information. The RMV may in its discretion audit all such documentation. The RMV will provide

the Requestor with written notice at least three (3) business days prior to said audit, which shall be performed with the reasonable cooperation of the Requestor. In the event the Requestor cannot provide a legitimate reason for accessing said data, said failure to do so may constitute a material breach under paragraph 12 of this Agreement. Furthermore, if the RMV's audit reveals inaccuracies or a violation of any provision of this Agreement, said violation or inaccuracies may be considered a material breach under paragraph 12 of the Agreement. If the Requestor does not have an office location in Massachusetts, upon request, the Requestor will forward all records to the RMV at the time and place designated by the RMV.

**B. Data Retention/Audit For eServices Portal or Business Portal Requestors:** The eServices Portal and Business Portal Requestor shall at all times adhere to the data retention and destruction requirements of M.G.L. Chapter 93I and the Massachusetts Public Records Law. Any data obtained from the RMV shall be shredded, destroyed or disposed of in compliance with Chapter 93I after its business purpose has expired. The RMV may track and audit all business transactions. The RMV may in its sole discretion require the requestor to explain and/or demonstrate its legitimate business purpose or permitted use for accessing the RMV's data for any particular transaction. Failure by the Requestor to do so may constitute a material breach under paragraph 12 of this Agreement. If the Requestor does not have an office location in Massachusetts, upon request the Requestor will forward all records to the RMV at the time and place designated by the RMV.

10. **Physical Security Of Data and Confidentiality:** The Requestor shall do the following:
- Ensure that RMV records are not visible to unauthorized individuals;
  - Shred or deposit RMV records into a locked shredder container when no longer needed;
  - Never knowingly obtain, disclose or use RMV records for a purpose not permitted under the DPPA. Requestor may be liable for impermissible dissemination of personal information to any individual to whom the personal information pertains;
  - Never misrepresent Requestor's identity or make a false statement in connection with a request for personal information with the intention of obtaining said information in a manner not authorized under this Agreement or the DPPA;
  - Never disseminate RMV records unless such dissemination is required by the Requestor's job duties;
  - Never use RMV records in the furtherance of an illegal act, including a violation of any criminal or civil laws;

11. **A. Background Checks For Requestors Who Receive Personal Information Contained in RMV Records and Data:**

- For Requestors Who Select SFTP, Web Services & eServices Option Under Paragraph 3: Prior to permitting access to the RMV's records and data, Requestor shall ensure through background checks that its employees, contractors and agents who have access to or who may view RMV data have not been convicted of a felony involving violence, dishonesty, deceit or indecency. A Requestor's employee, contractor or agent who has been convicted of such a felony shall not be qualified to access RMV data or view its data. For eServices Portal Administrators a background check will be conducted by the RMV.

- b. For Requestors Who Select the Business Portal Option under Paragraph 3: The RMV shall conduct background checks to ensure that the proposed employee, contractor and agent who will have access to or who may view RMV data has not been convicted of a felony involving violence, dishonesty, deceit or indecency. A Requestor's employee, contractor or agent who has been convicted of such a felony shall not be authorized to access the RMV database or view its data.
12. **Termination for Breach:** In addition to any termination of rights contained in this Agreement herein, the RMV may immediately terminate the Agreement and the Requestor's access to RMV data at any time, if the RMV determines in the exercise of its sole discretion, that the Requestor engaged in a material violation of any term of this Agreement, the DPPA, M.G.L. c. 93H, Executive Order 504, or any other law pertaining to the privacy of motor vehicle records. The RMV shall have no liability to the Requestor for terminating the Agreement under this provision.
13. **Right to Appeal:** The Requestor shall have the right to appeal the RMV's decision to terminate Requestor's access to RMV data pursuant to paragraph 12 above. Appeals should be made in writing and should be addressed to the Registrar of Motor Vehicles ("Registrar"). If no such appeal is made within 30 days of the termination, the termination shall be final. If the Requestor files an appeal within said 30 days period, the Registrar shall review the RMV's decision to terminate and shall make a final determination as to whether the terms of this Agreement were breached and, if so, whether the termination of access was appropriate. In making the final determination, the Registrar may consider any documentation proffered by the Requestor evidencing affirmative steps taken to prevent similar violations of this Agreement. The Registrar's decision is final and dispositive and no further appeal process is available.
14. **30 Day Termination:** Notwithstanding paragraph 5, this Agreement may be terminated by either party at any time upon thirty (30) days written notice. This agreement may be immediately terminated without advance notification upon any material breach of any covenant by either party, or if the performance of this Agreement by the RMV is made impossible or impractical, as determined in the sole reasonable judgment of the RMV, or if the requestor has not accessed the RMV's data base for a period of ninety(90) days, by any order of any Court, or any action of the Legislature of the Commonwealth of Massachusetts. Notice of termination shall be in writing signed by a duly-authorized representative of the terminating party and deposited with the United States Postal Service correctly addressed and postage prepaid.
15. **Indemnification:** The Requestor agrees to defend, hold harmless and indemnify the RMV, the Massachusetts Department of Transportation, the Commonwealth of Massachusetts and their employees and agents from any and all claims, actions, damages, or losses which may be brought or alleged against them for the negligent, improper, or unauthorized access, use or dissemination of the personal information contained in the RMV data. The Requestor shall indemnify and hold harmless the Commonwealth of Massachusetts and the Massachusetts Department of Transportation, and the RMV against any liability, claim loss, damage or expense, of every nature and kind in law or equity, arising out of or in connection with any misuse or misappropriation of any RMV Data obtained from the RMV; any failure of the Requestor to comply with any applicable provisions of State or Federal laws or regulations regarding privacy of motor vehicle records or data; any failure to safeguard and limit access to the RMV Data as



- required herein; and/or any other acts or omissions of the Requestor or its employees or agents in connection with the performance, exercise, or enjoyment of this Agreement, including without limitation reasonable attorney's fees and other costs of defending any such claim or action. The obligations under this paragraph shall survive the termination of this Agreement.
16. **Non-Assignment:** The Requestor shall not assign or in any way transfer any interest in this Agreement.
  17. **Non-Exclusivity:** The Requestor acknowledges that this Agreement is not an exclusive agreement. At its sole discretion the RMV may enter into agreements with other parties for the same or similar services as provided by this Agreement, on such terms and conditions as the RMV determines in its sole discretion.
  18. **Warranty:** The RMV makes no representation or warranty, express or implied, with respect to the accuracy of any RMV Data from a source other than the RMV. Therefore, except for acts or omissions that constitute gross negligence or willful misconduct by the Commonwealth of Massachusetts, the Massachusetts Department of Transportation, the RMV, their employees or agents, neither the Commonwealth of Massachusetts, the Massachusetts Department of Transportation, the RMV, or their employees or agents shall be liable to the Requestor for any costs, claims, liability, damages, expenses, lost production, or any other loss of any nature or kind, in law or equity, in connection with this Agreement, including but not limited to inaccurate, incomplete or unavailable RMV data.
  19. **Litigation Notice:** The Requestor shall immediately notify the Office of the General Counsel at the Massachusetts Department of Transportation in the event that it is sued or litigation is filed concerning the Requestor's use of RMV data.
  20. **Notice of Data Breach:** The Requestor shall immediately notify the Chief Information Security Office for the Massachusetts Department of Transportation at [InfoSecTeam@dot.state.ma.us](mailto:InfoSecTeam@dot.state.ma.us) in the event of a data breach or misuse of RMV data. The Requestor is responsible for all notifications and remediation pursuant to M.G.L. Chapter 93H.
  21. **Forum:** This agreement shall be construed under and governed by the laws and Executive Order 504 of the Commonwealth of Massachusetts.
  22. **Discrimination:** The Requestor shall not engage in any unlawful discrimination against any person based upon the RMV Data obtained pursuant to this Agreement, and the requestor agrees to comply with all applicable State and Federal laws, rules and regulations prohibiting discrimination in employment, including but not limit to 42 USC 12101, 28 CFR Part 35, 29 USC 791 et seq., Massachusetts General Laws Chapter 151 B and Chapter 272, §92A and §98 et seq. and Executive Orders 227, 237, and 246, or any amendments to such provisions.
  23. **Severability Clause:** In the event that any provision in this agreement shall be or become invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby and such provision shall be ineffective only to the extent of such invalidity, illegality or unenforceability.
  24. **Complete Instrument:** This Agreement constitutes the entire agreement of the parties and supersedes all other prior written or oral agreements between the parties with respect to subject matter hereof. This Agreement may be changed, modified or amended at any time only by an instrument in writing, signed by duly authorized representatives of both parties hereto.

25. **Notice:** Notice required or permitted by this Agreement shall be addressed to the address(s) as maintained by the requestor on their company profile on the RMV Web eServices or Business Portal or as follows:

To the RMV:

BY MAIL: MassDOT Registry of Motor Vehicles Division  
RMV IS Security  
25 Newport Avenue Extension  
Quincy, MA 02172

BY E-MAIL: RMVBUSINESSPARTNERS@state.ma.us

To NAME:

BY MAIL: FBI Boston  
201 Maple Street  
Chelsea, MA 02150

BY E-MAIL: BS\_Ops\_Center@ic.fbi.gov

Any party may change its address for the purposes of receipt of notices by providing written notice to the other party in accordance with this paragraph.

26. **Execution:** This Agreement may be executed in one or more counterparts, each of which will be deemed to be an original copy of this Agreement and all of which, when taken together, will be deemed to constitute one and the same agreement. The facsimile, email or other electronically delivered signatures of the parties shall be deemed to constitute original signatures, and facsimile or electronic copies hereof shall be deemed to constitute duplicate originals

IN WITNESS WHEREOF, the parties have hereto caused this instrument to be executed by their duly authorized officials or officers.

The Massachusetts Department  
Of Transportation, Registry of Motor  
Vehicles Division

NAME: FBI Boston

BY: 

BY: 

TITLE: Registrar

TITLE: Offices Services Supervisor

DATE: 2.2.18

DATE: 03/12/2018

SEC107\_0218



# **EXHIBIT 5**

**Jessica Lewis**

---

**From:** Kade Crockford  
**Sent:** Wednesday, February 20, 2019 3:14 PM  
**To:** MassDOT.RAO@state.ma.us  
**Cc:** Jessie Rossman; Emiliano Falcon  
**Subject:** Re: public records request  
**Attachments:** RMV-Face recognition Feb 2019.pdf

Hello again. My apologies. I accidentally sent you the wrong version of the request. Please use this version instead of the last one. I hereby withdraw my prior request and issue this one in its place.

Thanks.

Kade

---

**Kade Crockford**

Director, Technology for Liberty Program  
American Civil Liberties Union of Massachusetts  
211 Congress Street, Boston, MA 02110  
617.482.3170 x346 | [kcrockford@aclum.org](mailto:kcrockford@aclum.org)  
[aclum.org](http://aclum.org) | [privacysos.org/blog](http://privacysos.org/blog)

NSA: I'm a US person.

---

**From:** Kade Crockford  
**Sent:** Wednesday, February 20, 2019 2:47:30 PM  
**To:** MassDOT.RAO@state.ma.us  
**Cc:** Jessie Rossman; Emiliano Falcon  
**Subject:** public records request

Hello,

Please find a records request attached. I look forward to your response.

Thank you,  
Kade

---

**Kade Crockford**

Director, Technology for Liberty Program  
American Civil Liberties Union of Massachusetts

211 Congress Street, Boston, MA 02110  
617.482.3170 x346 | [kcrockford@aclum.org](mailto:kcrockford@aclum.org)  
[aclum.org](http://aclum.org) | [privacysos.org/blog](http://privacysos.org/blog)

NSA: I'm a US person.

February 20, 2019

Sent via email to [MassDOT.RAO@state.ma.us](mailto:MassDOT.RAO@state.ma.us)

William J. Doyle  
Records Access Officer  
Massachusetts Department of Transportation  
Commonwealth of Massachusetts

**Re: Public records request related to the use of facial-recognition searches**

Dear Mr. Doyle,

This is a request under the Massachusetts Public Records Law, G.L. c. 66, § 10, made on behalf of the American Civil Liberties Union Foundation of Massachusetts (“ACLU”).

The ACLU seeks records<sup>1</sup> relating to the Massachusetts Department of Transportation’s (“MassDOT”) use of facial-recognition<sup>2</sup> technology, including but not limited to records related to facial-recognition searches performed by the Registry of Motor Vehicles (“RMV”) and the RMV’s Enforcement Services division.

**Records requested**

The ACLU requests all such records created on or after January 1, 2016, including but not limited to:

1. Communications between any representative of MassDOT and any representative of any vendor offering any facial-recognition product or service.
2. Internal communications between representatives or employees of MassDOT relating to any facial-recognition product or service.
3. Documents relating to MassDOT’s purchasing or use of facial recognition, including but not limited to: purchase orders, RFPs, licensing agreements, invoices, and contracts (including non-disclosure agreements) related to any facial-recognition product or service.

---

<sup>1</sup> Throughout this request, the term “**records**” includes but is not limited to any paper or electronic information, reports, evaluations, memoranda, correspondence, letters, emails, charts, graphs, flyers, meeting agendas, meeting minutes, training materials, diagrams, forms, DVDs, tapes, CDs, notes, or other similar materials.

<sup>2</sup> In this letter, “**facial recognition**” means the automated or semi-automated process by which a person is identified or attempted to be identified based on the characteristics of his or her face.

4. Materials relating to how any facial-recognition product or service functions (or functions improperly), including e-mails, handouts, PowerPoint presentations, advertisements, or specification documents.
5. Manuals, policies, procedures, and practices governing the use or monitoring of a facial-recognition product or service or related information or databases. This request includes, but is not limited to:
  - a. Procedures for using, deleting, or retaining photos of subjects to be identified;
  - b. Materials identifying any sources of such photos, such as mobile devices, body cameras, surveillance videos, identification photos, or arrest photos;
  - c. Policies or procedures relating to the legal standard, if any, (e.g., probable cause, court order, relevance, consent) that is required before using any facial-recognition product or service.
  - d. Procedures the agency follows after a positive match, such as requiring independent or in-person verification;
  - e. Permitted uses of the information created from a positive match.
6. Training materials related to any facial-recognition product or service used by employees of MassDOT.
7. Records relating to any mobile application related to any facial-recognition product or service.
8. Records relating to any public process or debate about any facial-recognition product or service, including meeting agendas or minutes, public notice, analyses, or communications between MassDOT and elected leaders or county officials.
9. Any record containing the number of people flagged by any facial-recognition product or service as fraudulent or possibly fraudulent license applicants.
10. Any record containing the number of people flagged by any facial-recognition product or service as fraudulent or possibly fraudulent license applicants who appealed that determination, and were found to have not committed fraud.
11. All records containing information about the accuracy rates of any facial-recognition product or service in use by MassDOT.
12. All records containing information about the accuracy rates by gender, race, or other demographic characteristic of any facial-recognition product or service in use by MassDOT.
13. All internal audit reports or other documents produced subsequent to reviews of MassDOT's use of facial-recognition products or services.
14. Any document describing incidents of misuse or abuse of any facial-recognition product or service.
15. Any records documenting each instance in which the RMV drivers license database has been searched or examined using facial-recognition technology by the Massachusetts State Police or on behalf of any law enforcement entity. Please include records showing

how many times these searches or examinations were performed on behalf of each agency, and if possible, the documented reason for the search or examination.

Because this request involves a matter of public concern and because it is made on behalf of a nonprofit organization, we ask that you waive any fees. ACLU is a nonprofit §501(c)(3) organization dedicated to the protection of civil rights and liberties for all persons in the Commonwealth of Massachusetts. As the state's affiliate of the American Civil Liberties Union, the ACLU of Massachusetts is part of a nationwide network of advocates dedicated to defending and expanding the civil liberties of all.

If you decide not to waive fees, we request that you permit us to examine, at our election, the responsive documents before deciding which portions to copy. We would prefer the documents in electronic format.

Should you determine that some portion of the documents requested are exempt from disclosure, please release any reasonably segregable portions that are not exempt. In addition, please note the applicable statutory exemption and explain why it applies to the redacted portions. As you know, a custodian of public records shall comply with a request within ten days after receipt.

If you have questions about this request, please contact me at (617) 482-3170 x346 or [kcrockford@aclum.org](mailto:kcrockford@aclum.org).

Thank you for your assistance. We look forward to your response.

Sincerely,



Kade Crockford  
Director  
Technology for Liberty Program  
ACLU of Massachusetts







**Jessica Lewis**

---

**From:** Kade Crockford  
**Sent:** Thursday, April 11, 2019 3:54 PM  
**To:** Doyle, William (DOT)  
**Cc:** Jessie Rossman; Jessica Lewis; Emiliano Falcon  
**Subject:** Re: Public Records Request (MassDOT) :: P000202-021519  
**Attachments:** RMV-Face recognition Feb 2019.pdf

Mr. Doyle, can you please let me know when we can expect a response to this request? It's been well over the ten days allowed by state law.

I have attached the request again for your convenience.

Thank you.

Kade

**Kade Crockford**

Director, Technology for Liberty Program  
American Civil Liberties Union of Massachusetts  
211 Congress Street, Boston, MA 02110  
617.482.3170 x346 | [kcrockford@aclum.org](mailto:kcrockford@aclum.org)  
[aclum.org](http://aclum.org) | [privacysos.org/blog](http://privacysos.org/blog)

NSA: I'm a US person.

---

**From:** Kade Crockford  
**Sent:** Monday, March 25, 2019 9:31:32 AM  
**To:** Doyle, William (DOT)  
**Cc:** Jessie Rossman; Jessica Lewis  
**Subject:** Re: Public Records Request (MassDOT) :: P000202-021519

I've attached the request I'm talking about. I never received a tracking number for this request.

**Kade Crockford**

Director, Technology for Liberty Program  
American Civil Liberties Union of Massachusetts  
211 Congress Street, Boston, MA 02110  
617.482.3170 x346 | [kcrockford@aclum.org](mailto:kcrockford@aclum.org)  
[aclum.org](http://aclum.org) | [privacysos.org/blog](http://privacysos.org/blog)

NSA: I'm a US person.

---

**From:** Doyle, William (DOT) <william.doyle@state.ma.us>  
**Sent:** Monday, March 25, 2019 9:18:36 AM  
**To:** Kade Crockford  
**Cc:** Jessie Rossman; Jessica Lewis  
**Subject:** RE: Public Records Request (MassDOT) :: P000202-021519

Kade,

Can you let me know the reference number of the request? I was looking at the P000202 number that was in your original subject line.

Sincerely,

**William J. Doyle, Esq.**

**Records Access Officer/***massDOT*

Office of the General Counsel  
(857) 368-8752

**From:** Kade Crockford <kcrockford@aclum.org>  
**Sent:** Monday, March 25, 2019 8:45 AM  
**To:** Doyle, William (DOT) <William.Doyle@dot.state.ma.us>  
**Cc:** Jessie Rossman <JRossman@aclum.org>; Jessica Lewis <jlewis@aclum.org>  
**Subject:** Re: Public Records Request (MassDOT) :: P000202-021519

Thanks. I'm talking about a separate request.

---

Kade Crockford  
Director  
Technology for Liberty Program  
ACLU of Massachusetts

On Mon, Mar 25, 2019 at 8:44 AM -0400, "Doyle, William (DOT)" <[william.doyle@state.ma.us](mailto:william.doyle@state.ma.us)> wrote:

Kade,

Please check your junk mail folder to be sure you did not receive our response from March 19 at 12:26 PM (it will be from GovQA). I had included an additional Memorandum of Understanding responsive to your request.

Sincerely,

**William J. Doyle, Esq.**

**Records Access Officer/***massDOT*

Office of the General Counsel  
(857) 368-8752

**From:** Kade Crockford <[kcrockford@aclum.org](mailto:kcrockford@aclum.org)>

**Sent:** Friday, March 22, 2019 3:02 PM

**To:** MassDOT Public Records Center <[massachusettsdot@mycusthelp.net](mailto:massachusettsdot@mycusthelp.net)>; Jessie Rossman <[JRossman@aclum.org](mailto:JRossman@aclum.org)>; Doyle, William (DOT) <[William.Doyle@dot.state.ma.us](mailto:William.Doyle@dot.state.ma.us)>; Jessica Lewis <[jlewis@aclum.org](mailto:jlewis@aclum.org)>

**Subject:** Re: Public Records Request (MassDOT) :: P000202-021519

Hello Mr. Doyle,

I just called your office and left you a message inquiring about when I can expect to receive a response to my February 20 records request to MassDOT. I've attached that request here for your convenience.

As you know, custodians of public records are required by law to respond to requests within 10 business days. It has been over a month.

Please let me know when I can expect to receive these records.

Thanks,  
Kade

---

**Kade Crockford**

Director, Technology for Liberty Program  
American Civil Liberties Union of Massachusetts  
211 Congress Street, Boston, MA 02110  
617.482.3170 x346 | [kcrockford@aclum.org](mailto:kcrockford@aclum.org)  
[aclum.org](http://aclum.org) | [privacysos.org/blog](http://privacysos.org/blog)

NSA: I'm a US person.

---

**From:** Kade Crockford

**Sent:** Tuesday, March 19, 2019 1:22:59 PM

**To:** MassDOT Public Records Center; Jessie Rossman

**Subject:** Re: Public Records Request (MassDOT) :: P000202-021519

Thank you. I'm still waiting to receive a response to my February 20, 2019 records request.

I'm attaching it again for your convenience. Thanks.

Kade

---

**Kade Crockford**

Director, Technology for Liberty Program  
American Civil Liberties Union of Massachusetts  
211 Congress Street, Boston, MA 02110  
617.482.3170 x346 | [kcrockford@aclum.org](mailto:kcrockford@aclum.org)  
[aclum.org](http://aclum.org) | [privacysos.org/blog](http://privacysos.org/blog)

NSA: I'm a US person.

---

**From:** MassDOT Public Records Center <[massachusettsdot@mycusthelp.net](mailto:massachusettsdot@mycusthelp.net)>  
**Sent:** Tuesday, March 19, 2019 12:26:59 PM  
**To:** Kade Crockford  
**Subject:** Public Records Request (MassDOT) :: P000202-021519

--- Please respond above this line ---

March 19, 2019

Kade Crockford

Re: Public Records Request: "I'd like to follow up and ask the RMV to perform the search again. It's my understanding that there are other memoranda of agreement with law enforcement agencies. Can you please perform another search?" (The relevant portion of the request you reference was for ""All memoranda of understanding and/or memoranda of agreement between the Registry of Motor Vehicles and any law enforcement agency, including but not limited to the Massachusetts State Police and the Federal Bureau of Investigation."")

**Our Case No.: P000202-021519**

Dear Kade Crockford,

We have reviewed the RMV records and located an additional Memorandum of Understanding which would be responsive to your request; below is a link to that record (see "My Request Center"). Please be advised that a portion of this public record seeks information that is exempt from disclosure under Massachusetts General Laws Chapter 4, Section 7(26)(n) which exempts "records, including, but not limited to, blueprints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, or any other records relating to the security or safety of persons or buildings, structures, facilities, utilities, transportation, cyber security or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the record custodian, subject to review by the supervisor of public records under subsection (c) of section 10 of chapter 66, is likely to jeopardize public safety or cyber security". In this case, MassDOT's records custodian has determined in its judgment that an unredacted release of the record you have requested is likely to increase the threat of a cyber-security incident.

Please be advised that in the case of a denial of access to records, you have the right to an

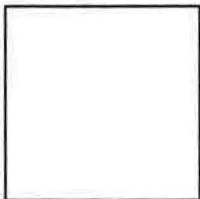
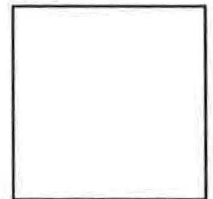
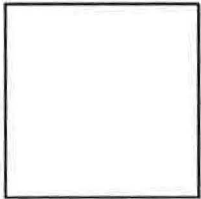
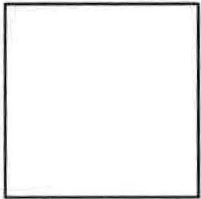
administrative appeal to the Supervisor of Records, pursuant to 950CMR 32.08(1) (the Code of Massachusetts Regulations), and the right to seek judicial review by commencing an action in the Superior Court. Accordingly, we are closing our file.

My Request Center

If you need additional information, or there is any other way we can assist you, please respond through the portal or contact our general public records line at (857) 368-8760. Please refer to Case No.: P000202-021519.

Sincerely,

William J. Doyle  
Records Access Officer  
Office of the General Counsel



# **EXHIBIT 6**

## Jessica Lewis

---

**From:** Emiliano Falcon  
**Sent:** Wednesday, April 24, 2019 12:21 PM  
**To:** MassDOT.RAO@state.ma.us  
**Cc:** Kade Crockford; Jessie Rossman; Jessica Lewis  
**Subject:** ACLU Public Records Request  
**Attachments:** ACLU PRR 4-24.pdf

Dear Mr. Doyle,

Please see the public records request attached.

Best regards,

Emiliano

-----

**Emiliano Falcon**

Pronouns: he, him, his

Technology and Civil Liberties Policy Counsel  
Technology for Liberty Program  
American Civil Liberties Union of Massachusetts  
211 Congress Street, Boston, MA 02110  
617.482.3170 x402 | [efalcon@aclum.org](mailto:efalcon@aclum.org)

[Website](#) | [Twitter](#) | [Facebook](#) | [Instagram](#) | [Youtube](#)





April 24, 2019

Sent via email to [MassDOT.RAO@state.ma.us](mailto:MassDOT.RAO@state.ma.us)

William J. Doyle  
Record Access Officer  
Massachusetts Department of Transportation  
Commonwealth of Massachusetts

**Re: Public records request related to the sharing of information by the Massachusetts Department of Transportation**

Dear Mr. Doyle:

On February 20, 2019, the American Civil Liberties Union Foundation of Massachusetts ("ACLU") submitted a public records request to your office, requesting documents relating to the Massachusetts Department of Transportation's ("MassDOT") use of facial recognition technology. To date, we have not received a response. We ask that you promptly provide the requested records, which are now well-past the statutory deadline for compliance.

In addition, today we file this related request under the Massachusetts Public Records Law, G.L. c. 66 § 10. Specifically ACLU seeks records<sup>1</sup> pertaining to the sharing of information between the MassDOT's divisions and departments, including but not limited to the Registry of Motor Vehicles ("RMV"), and other state and local agencies, federal agencies, and private actors. In particular, we are requesting records that show how the MassDOT shares driver's licenses and other RMV-issued identification cards photos and pictures ("ID pictures"), gives access to the databases where ID pictures are stored, or otherwise makes ID pictures available. We also seek records pertaining to requests for access to the ID pictures, in cases where the requests were denied.

**Records requested**

The ACLU requests all such records created on or after January 1, 2016, including but not limited to:

1. All memoranda of understanding, memoranda of agreement, agreements for services, non-disclosure agreements and/or any other type of agreement (collectively referred as "agreements") by which the MassDOT and its agents share ID pictures, give access to the databases where ID pictures are stored, or otherwise make ID pictures available. This request includes agreements with state agencies, local agencies, federal agencies, private actors or companies;

---

<sup>1</sup> Throughout this request, the term "records" includes but is not limited to any paper or electronic information, reports, evaluations, memoranda, correspondence, letters, emails, charts, graphs, flyers, meeting agendas, meeting minutes, training materials, diagrams, forms, DVDs, tapes, CDs, notes, or other similar materials.





## Massachusetts

2. Manuals, policies, procedures, and practices governing the sharing of ID pictures with, or granting access to the databases where ID pictures are stored to, other state agencies, local agencies, federal agencies, private actors or companies;
3. Records showing the state agencies, local agencies, federal agencies, private actors or companies that requested the sharing of ID pictures or access to databases where ID pictures are stored, and how many times they each made such requests;
4. Records showing how many times the MassDOT shared ID pictures with, or gave access to the databases where ID pictures are stored to, other state agencies, local agencies, federal agencies, private actors or companies;
5. Records showing how many times the MassDOT did not share ID pictures with, or denied access to the databases where ID pictures are stored to, other state agencies, local agencies, federal agencies, private actors or companies;

Because this request involves a matter of public concern and because it is made on behalf of a nonprofit organization, we ask that you waive any fees. ACLU is a nonprofit §501(c)(3) organization dedicated to the protection of civil rights and liberties for all persons in the Commonwealth of Massachusetts. As the state's affiliate of the American Civil Liberties Union, the ACLU of Massachusetts is part of a nationwide network of advocates dedicated to defending and expanding the civil liberties of all.

If you decide not to waive fees, we request that you permit us to examine, at our election, the responsive documents before deciding which portions to copy. We would prefer the documents in electronic format.

Should you determine that some portion of the documents requested are exempt from disclosure, please release any reasonably segregable portions that are not exempt. In addition, please note the applicable statutory exemption and explain why it applies to the redacted portions. As you know, a custodian of public records shall comply with a request within ten days after receipt.

If you have questions about this request, please contact me at [kcrockford@aclum.org](mailto:kcrockford@aclum.org).

Thank you for your assistance. We look forward to your response.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kade Crockford".

Kade Crockford  
Director  
Technology for Liberty Program  
ACLU of Massachusetts



## Jessica Lewis

---

**From:** Emiliano Falcon  
**Sent:** Wednesday, April 24, 2019 12:26 PM  
**To:** Kade Crockford; Jessica Lewis; Jessie Rossman  
**Subject:** FW: MassDOT RAO: Your request has been received

-----  
Emiliano Falcon  
Pronouns: he, him, his  
Technology and Civil Liberties Policy Counsel

**From:** PublicRecords, MassDOT (DOT) [mailto:massdot.publicrecords2@state.ma.us]  
**Sent:** Wednesday, April 24, 2019 12:23 PM  
**To:** Emiliano Falcon <efalcon@aclum.org>  
**Subject:** MassDOT RAO: Your request has been received

Please note that MassDOT looks forward to providing you the information you seek under the public records law.

You may submit your public records requests in several ways:

**By Online Portal:**

Please [visit the online portal](#) and follow the directions. This new web portal will allow you to make requests, receive notifications, check the status and receive your records all from within a dedicated system. Like most web-based systems, you will initially have to create a user name and password, but that will only be a one-time requirement.

**By Fax:**

(857) 368-0615

**By U.S. Mail, or In-Person:**

Public Records Requests  
MassDOT Office of the General Counsel  
10 Park Plaza, Suite 3510  
Boston, MA 02116

**By Email:**

If you would prefer to make your request by standard email, you may reply to this email with your request.

We look forward to assisting you with your public records request.