

From: JudithReardon.Riley@dot.state.ma.us
To: [Deveney, Erin \(DOT\)](mailto:Deveney.Erin@dot.state.ma.us); [Lavoie, Sara \(DOT\)](mailto:Lavoie.Sara@dot.state.ma.us)
Cc: [Goddard, Jacquelyn \(DOT\)](mailto:Goddard.Jacquelyn@dot.state.ma.us)
Bcc: [Riley, Judith \(DOT\)](mailto:Riley.Judith@dot.state.ma.us)
Subject: Fwd: Draft response to Herald Re: Facial Recognition
Date: Thursday, June 6, 2019 7:40:06 PM

Hi Registrar and Sara,

Do you have any comments on Dave's draft below?

Thanks,

Judi

Sent from my iPhone

Begin forwarded message:

From: "Riley, Judith (DOT)" <JudithReardon.Riley@dot.state.ma.us>
Date: June 6, 2019 at 5:34:55 PM EDT
To: "Procopio, David (POL)" <david.procopio@pol.state.ma.us>
Cc: "Deveney, Erin (DOT)" <Erin.Deveney@dot.state.ma.us>, "Goddard, Jacquelyn (DOT)" <Jacquelyn.Goddard@dot.state.ma.us>
Subject: RE: Draft response to Herald Re: Facial Recognition

Hi Dave,

I am looping in Registrar Deveney.

Thanks,

Judi

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>
Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.

Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants

remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Riley, Judith \(DOT\)](#)
To: [Deveney, Erin \(DOT\)](#); [Lavoie, Sara \(DOT\)](#)
Cc: [Goddard, Jacquelyn \(DOT\)](#)
Subject: Fwd: Draft response to Herald Re: Facial Recognition
Date: Thursday, June 6, 2019 7:40:07 PM

Hi Registrar and Sara,

Do you have any comments on Dave's draft below?

Thanks,

Judi

Sent from my iPhone

Begin forwarded message:

From: "Riley, Judith (DOT)" <JudithReardon.Riley@dot.state.ma.us>
Date: June 6, 2019 at 5:34:55 PM EDT
To: "Procopio, David (POL)" <david.procopio@pol.state.ma.us>
Cc: "Deveney, Erin (DOT)" <Erin.Deveney@dot.state.ma.us>, "Goddard, Jacquelyn (DOT)" <Jacquelyn.Goddard@dot.state.ma.us>
Subject: RE: Draft response to Herald Re: Facial Recognition

Hi Dave,

I am looping in Registrar Deveney.

Thanks,

Judi

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>
Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.

Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial

Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: Jacquelyn.Goddard@dot.state.ma.us
To: [Riley, Judith \(DOT\)](mailto:Riley.Judith@dot.state.ma.us)
Cc: [Deveney, Erin \(DOT\)](mailto:Deveney.Erin@dot.state.ma.us); [Lavoie, Sara \(DOT\)](mailto:Lavoie.Sara@dot.state.ma.us)
Bcc: [Garrity, Rob \(DOT\)](mailto:Garrity.Rob@dot.state.ma.us); [Marvin, Patrick \(DOT\)](mailto:Marvin.Patrick@dot.state.ma.us); [Huber, Maxwell \(DOT\)](mailto:Huber.Maxwell@dot.state.ma.us); Sarah Finlaw
Subject: deadline Friday—Herald Facial Recognition
Date: Thursday, June 6, 2019 8:12:39 PM

Judi and Registrar- please note I just talked to this reporter. She does not need answers tonight. Judi will draft comment in the morning and we can get reporter comment by 11 am Friday.
Thanks

Jacquelyn Goddard
Communications Office
Massachusetts Department of Transportation

On Jun 6, 2019, at 7:40 PM, Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us> wrote:

Hi Registrar and Sara,

Do you have any comments on Dave's draft below?

Thanks,

Judi

Sent from my iPhone

Begin forwarded message:

From: "Riley, Judith (DOT)" <JudithReardon.Riley@dot.state.ma.us>
Date: June 6, 2019 at 5:34:55 PM EDT
To: "Procopio, David (POL)" <david.procopio@pol.state.ma.us>
Cc: "Deveney, Erin (DOT)" <Erin.Deveney@dot.state.ma.us>, "Goddard, Jacquelyn (DOT)" <Jacquelyn.Goddard@dot.state.ma.us>
Subject: RE: Draft response to Herald Re: Facial Recognition

Hi Dave,

I am looping in Registrar Deveney.

Thanks,

Judi

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>

Sent: Thursday, June 6, 2019 5:31 PM

To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>

Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.

Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and

striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Goddard, Jacquelyn \(DOT\)](#)
To: [Riley, Judith \(DOT\)](#)
Cc: [Deveney, Erin \(DOT\)](#); [Lavoie, Sara \(DOT\)](#)
Subject: deadline Friday—Herald Facial Recognition
Date: Thursday, June 6, 2019 8:12:41 PM

Judi and Registrar- please note I just talked to this reporter. She does not need answers tonight. Judi will draft comment in the morning and we can get reporter comment by 11 am Friday.
Thanks

Jacquelyn Goddard
Communications Office
Massachusetts Department of Transportation

On Jun 6, 2019, at 7:40 PM, Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us> wrote:

Hi Registrar and Sara,

Do you have any comments on Dave's draft below?

Thanks,

Judi

Sent from my iPhone

Begin forwarded message:

From: "Riley, Judith (DOT)" <JudithReardon.Riley@dot.state.ma.us>
Date: June 6, 2019 at 5:34:55 PM EDT
To: "Procopio, David (POL)" <david.procopio@pol.state.ma.us>
Cc: "Deveney, Erin (DOT)" <Erin.Deveney@dot.state.ma.us>, "Goddard, Jacquelyn (DOT)" <Jacquelyn.Goddard@dot.state.ma.us>
Subject: RE: Draft response to Herald Re: Facial Recognition

Hi Dave,

I am looping in Registrar Deveney.

Thanks,

Judi

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>

Sent: Thursday, June 6, 2019 5:31 PM

To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>

Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.

Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and

striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Lavoie, Sara \(DOT\)](#)
To: [Goddard, Jacquelyn \(DOT\)](#); [Riley, Judith \(DOT\)](#)
Cc: [Deveney, Erin \(DOT\)](#)
Subject: RE: deadline Friday—Herald Facial Recognition
Date: Friday, June 7, 2019 9:35:18 AM

Hi—just trying to get all asks in one place, looks like 2 items for us.

1) Questions for RMV to answer – I drafted some responses below. Needs work!

1) I'm assuming the RMV makes these photos available to police if they ask for it? **The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them and the identity of the individuals before them.**

Are there any steps the RMV takes to protect the privacy of individuals? **The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)**

Also, besides the RMV, does the DOT use facial recognition in any way? **No.**

2) Any RMV comments to Procopio statement. **My suggestion/edits are highlighted.**

The Massachusetts State Police utilize **(might change utilize to may access)** facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected **driver's license and identity** fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit **(suggest changing to hit to potential match, not hit)** in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general

investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below. **I have no comment on the examples**

From: Goddard, Jacquelyn (DOT)
Sent: Thursday, June 06, 2019 8:13 PM
To: Riley, Judith (DOT)
Cc: Deveney, Erin (DOT); Lavoie, Sara (DOT)
Subject: deadline Friday—HeraldFacial Recognition

Judi and Registrar- please note I just talked to this reporter. She does not need answers tonight. Judi will draft comment in the morning and we can get reporter comment by 11 am Friday.
Thanks

Jacquelyn Goddard
Communications Office
Massachusetts Department of Transportation

On Jun 6, 2019, at 7:40 PM, Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us> wrote:

Hi Registrar and Sara,

Do you have any comments on Dave's draft below?

Thanks,

Judi

Sent from my iPhone

Begin forwarded message:

From: "Riley, Judith (DOT)" <JudithReardon.Riley@dot.state.ma.us>
Date: June 6, 2019 at 5:34:55 PM EDT
To: "Procopio, David (POL)" <david.procopio@pol.state.ma.us>
Cc: "Deveney, Erin (DOT)" <Erin.Deveney@dot.state.ma.us>, "Goddard, Jacquelyn (DOT)" <Jacquelyn.Goddard@dot.state.ma.us>
Subject: RE: Draft response to Herald Re: Facial Recognition

Hi Dave,

I am looping in Registrar Deveney.

Thanks,

Judi

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>;
Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara
(DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT)
<JudithReardon.Riley@dot.state.ma.us>
Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.
Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the*

investigation must be determined through further investigation.

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Goddard, Jacquelyn \(DOT\)](#)
To: [Procopio, David \(POL\)](#); [Moss, Brendan C. \(GOV\)](#)
Cc: [Finlaw, Sarah \(GOV\)](#); [Riley, Judith \(DOT\)](#); [Marvin, Patrick \(DOT\)](#); [Garrity, Rob \(DOT\)](#); [Huber, Maxwell \(DOT\)](#); [McGlinchey, Madison \(DOT\)](#)
Subject: FW: deadline at noon today —Herald story on Facial Recognition
Date: Friday, June 7, 2019 9:43:37 AM

David and Brendan,

Re: Herald questions on facial recognition use.

Please see below for the RMV suggested edits to David's draft comment and in red font RMV answers to RMV questions.

Boston Herald needs comment by noon.

Thanks,
Jacque

DRAFT at 9:45 a.m.

Questions for RMV to answer:

Q: I'm assuming the RMV makes these photos available to police if they ask for it?
The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.

Q: Are there any steps the RMV takes to protect the privacy of individuals? **The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)**

Q: Also, besides the RMV, does the DOT use facial recognition in any way?
MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal driver privacy protection act and policy guidelines.

2) Any RMV comments to David Procopio statement?. RMV suggested edits in yellow highlights.

The Massachusetts State Police utilize **(might change utilize to may access)** facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected **driver's license and identity** fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit **(suggest changing to hit to potential match,**

not hit) in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>
Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.
Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to

investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Goddard, Jacquelyn \(DOT\)](#)
To: [Lavoie, Sara \(DOT\)](#); [Riley, Judith \(DOT\)](#)
Cc: [Deveney, Erin \(DOT\)](#)
Subject: RE: deadline Friday—HeraldFacial Recognition
Date: Friday, June 7, 2019 9:47:03 AM

Thanks Sara.

Sending this outside the building now to be review.

We appreciate your help.

From: Lavoie, Sara (DOT)
Sent: Friday, June 07, 2019 9:35 AM
To: Goddard, Jacquelyn (DOT); Riley, Judith (DOT)
Cc: Deveney, Erin (DOT)
Subject: RE: deadline Friday—HeraldFacial Recognition

Hi—just trying to get all asks in one place, looks like 2 items for us.

1) Questions for RMV to answer – I drafted some responses below. Needs work!

1) I'm assuming the RMV makes these photos available to police if they ask for it? **The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them and the identity of the individuals before them.**

Are there any steps the RMV takes to protect the privacy of individuals? **The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)**

Also, besides the RMV, does the DOT use facial recognition in any way? **No.**

2) Any RMV comments to Procopio statement. **My suggestion/edits are highlighted.**

The Massachusetts State Police utilize **(might change utilize to may access)** facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected **driver's license and identity** fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit **(suggest changing to hit to potential match, not hit)** in and of itself is not a positive identification. Rather, it is an investigative lead that

requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below. **I have no comment on the examples**

From: Goddard, Jacquelyn (DOT)
Sent: Thursday, June 06, 2019 8:13 PM
To: Riley, Judith (DOT)
Cc: Deveney, Erin (DOT); Lavoie, Sara (DOT)
Subject: deadline Friday—HeraldFacial Recognition

Judi and Registrar- please note I just talked to this reporter. She does not need answers tonight. Judi will draft comment in the morning and we can get reporter comment by 11 am Friday.
Thanks

Jacquelyn Goddard
Communications Office
Massachusetts Department of Transportation

On Jun 6, 2019, at 7:40 PM, Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us> wrote:

Hi Registrar and Sara,

Do you have any comments on Dave's draft below?

Thanks,

Judi

Sent from my iPhone

Begin forwarded message:

From: "Riley, Judith (DOT)" <JudithReardon.Riley@dot.state.ma.us>
Date: June 6, 2019 at 5:34:55 PM EDT
To: "Procopio, David (POL)" <david.procopio@pol.state.ma.us>
Cc: "Deveney, Erin (DOT)" <Erin.Deveney@dot.state.ma.us>, "Goddard, Jacquelyn (DOT)" <Jacquelyn.Goddard@dot.state.ma.us>

Subject: RE: Draft response to Herald Re: Facial Recognition

Hi Dave,

I am looping in Registrar Deveney.

Thanks,

Judi

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>
Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.

Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is

not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the

Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Procopio, David \(POL\)](#)
To: [Goddard, Jacquelyn \(DOT\)](#)
Cc: [Moss, Brendan C. \(GOV\)](#); [Finlaw, Sarah \(GOV\)](#); [Riley, Judith \(DOT\)](#); [Marvin, Patrick \(DOT\)](#); [Garrity, Rob \(DOT\)](#); [Huber, Maxwell \(DOT\)](#); [McGlinchey, Madison \(DOT\)](#)
Subject: Re: deadline at noon today —Herald story on Facial Recognition
Date: Friday, June 7, 2019 10:11:33 AM

Thank you

Sent from my iPhone

On Jun 7, 2019, at 9:43 AM, Goddard, Jacquelyn (DOT)
<Jacquelyn.Goddard@dot.state.ma.us> wrote:

David and Brendan,
Re: Herald questions on facial recognition use.
Please see below for the RMV suggested edits to David's draft comment and in red font RMV answers to RMV questions.

Boston Herald needs comment by noon.

Thanks,
Jacque

DRAFT at 9:45 a.m.

Questions for RMV to answer:

Q: I'm assuming the RMV makes these photos available to police if they ask for it? **The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.**

Q: Are there any steps the RMV takes to protect the privacy of individuals? **The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)**

Q: Also, besides the RMV, does the DOT use facial recognition in any way? **MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal driver privacy protection act and policy guidelines.**

2) Any RMV comments to David Procopio statement?. RMV suggested edits in yellow highlights.

The Massachusetts State Police utilize **(might change utilize to may access)** facial recognition technology, when applicable, to further criminal investigations,

primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected **driver's license and identity** fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit (**suggest changing to hit to potential match, not hit**) in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

From: Procopio, David (POL)
<david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT)
<Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>
Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.

Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP

analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell

phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham

Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Goddard, Jacquelyn \(DOT\)](#)
To: [Riley, Judith \(DOT\)](#)
Subject: FW: deadline at noon today —Herald story on Facial Recognition
Date: Friday, June 7, 2019 10:25:16 AM

David indicated that he approves his comment edits.

From: Procopio, David (POL)
Sent: Friday, June 07, 2019 10:12 AM
To: Goddard, Jacquelyn (DOT)
Cc: Moss, Brendan C. (GOV); Finlaw, Sarah (GOV); Riley, Judith (DOT); Marvin, Patrick (DOT); Garrity, Rob (DOT); Huber, Maxwell (DOT); McGlinchey, Madison (DOT)
Subject: Re: deadline at noon today —Herald story on Facial Recognition

Thank you

Sent from my iPhone

On Jun 7, 2019, at 9:43 AM, Goddard, Jacquelyn (DOT)
<Jacquelyn.Goddard@dot.state.ma.us> wrote:

David and Brendan,
Re: Herald questions on facial recognition use.
Please see below for the RMV suggested edits to David's draft comment and in red font RMV answers to RMV questions.

Boston Herald needs comment by noon.

Thanks,
Jacque

DRAFT at 9:45 a.m.

Questions for RMV to answer:

Q: I'm assuming the RMV makes these photos available to police if they ask for it? **The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.**

Q: Are there any steps the RMV takes to protect the privacy of individuals? **The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)**

Q: Also, besides the RMV, does the DOT use facial recognition in any way? **MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal driver privacy protection act and policy guidelines.**

2) Any RMV comments to David Procopio statement?. RMV suggested edits in yellow highlights.

The Massachusetts State Police utilize (might change utilize to may access) facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected driver's license and identity fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit (suggest changing to hit to potential match, not hit) in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

From: Procopio, David (POL)
<david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT)
<Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>
Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.

Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have

active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four

members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Riley, Judith \(DOT\)](#)
To: [Goddard, Jacquelyn \(DOT\)](#)
Subject: RE: deadline at noon today —Herald story on Facial Recognition
Date: Friday, June 7, 2019 10:31:00 AM

Thanks.

From: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Sent: Friday, June 7, 2019 10:25 AM
To: Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>
Subject: FW: deadline at noon today —Herald story on Facial Recognition

David indicated that he approves his comment edits.

From: Procopio, David (POL)
Sent: Friday, June 07, 2019 10:12 AM
To: Goddard, Jacquelyn (DOT)
Cc: Moss, Brendan C. (GOV); Finlaw, Sarah (GOV); Riley, Judith (DOT); Marvin, Patrick (DOT); Garrity, Rob (DOT); Huber, Maxwell (DOT); McGlinchey, Madison (DOT)
Subject: Re: deadline at noon today —Herald story on Facial Recognition

Thank you

Sent from my iPhone

On Jun 7, 2019, at 9:43 AM, Goddard, Jacquelyn (DOT)
<Jacquelyn.Goddard@dot.state.ma.us> wrote:

David and Brendan,
Re: Herald questions on facial recognition use.
Please see below for the RMV suggested edits to David's draft comment and in red font RMV answers to RMV questions.

Boston Herald needs comment by noon.

Thanks,
Jacque

DRAFT at 9:45 a.m.

Questions for RMV to answer:

Q: I'm assuming the RMV makes these photos available to police if they ask for it? **The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.**

Q: Are there any steps the RMV takes to protect the privacy of individuals? **The dissemination of RMV held images is strictly controlled by**

the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)

Q: Also, besides the RMV, does the DOT use facial recognition in any way? **MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal driver privacy protection act and policy guidelines.**

2) Any RMV comments to David Procopio statement?. RMV suggested edits in yellow highlights.

The Massachusetts State Police utilize **(might change utilize to may access)** facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected **driver's license and identity** fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit **(suggest changing to hit to potential match, not hit)** in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

From: Procopio, David (POL)
<david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM

To: Goddard, Jacquelyn (DOT)
<Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick
(DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT)
<Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT)
<JudithReardon.Riley@dot.state.ma.us>

Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.
Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an*

investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of

them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to

Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Riley, Judith \(DOT\)](#)
To: [Procopio, David \(POL\)](#); [Moss, Brendan C. \(GOV\)](#)
Cc: [Finlaw, Sarah \(GOV\)](#); [Garrity, Rob \(DOT\)](#)
Subject: deadline at noon today —Herald story on Facial Recognition
Date: Friday, June 7, 2019 10:35:10 AM

Hi David,

Do you have any comments on the RMV's draft responses below?

Questions for RMV to answer:

I'm assuming the RMV makes these photos available to police if they ask for it?

The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.

Are there any steps the RMV takes to protect the privacy of individuals?

The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)

Also, besides the RMV, does the DOT use facial recognition in any way?

MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal driver privacy protection act and policy guidelines.

Thanks,

Judi

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Sent: Friday, June 7, 2019 10:12 AM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Cc: Moss, Brendan C. (GOV) <Brendan.C.Moss@MassMail.State.MA.US>; Finlaw, Sarah (GOV) <sarah.finlaw@state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Garrity, Rob (DOT) <rob.garrity@state.ma.us>; Huber, Maxwell (DOT) <Maxwell.Huber@dot.state.ma.us>; McGlinchey, Madison (DOT) <Madison.McGlinchey@dot.state.ma.us>
Subject: Re: deadline at noon today —Herald story on Facial Recognition

Thank you

Sent from my iPhone

On Jun 7, 2019, at 9:43 AM, Goddard, Jacquelyn (DOT)

<Jacquelyn.Goddard@dot.state.ma.us> wrote:

David and Brendan,
Re: Herald questions on facial recognition use.
Please see below for the RMV suggested edits to David's draft comment and in red font RMV answers to RMV questions.

Boston Herald needs comment by noon.

Thanks,
Jacque

DRAFT at 9:45 a.m.

Questions for RMV to answer:

Q: I'm assuming the RMV makes these photos available to police if they ask for it? **The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.**

Q: Are there any steps the RMV takes to protect the privacy of individuals? **The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)**

Q: Also, besides the RMV, does the DOT use facial recognition in any way? **MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal driver privacy protection act and policy guidelines.**

2) Any RMV comments to David Procopio statement?. RMV suggested edits in yellow highlights.

The Massachusetts State Police utilize **(might change utilize to may access)** facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected **driver's license and identity** fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit (**suggest changing to hit to potential match, not hit**) in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

From: Procopio, David (POL)
<david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT)
<Jacquelyn.Goddard@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Lavoie, Sara (DOT) <Sara.Lavoie@dot.state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>
Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.
Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the

investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the

investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Procopio, David \(POL\)](#)
To: [Riley, Judith \(DOT\)](#)
Cc: [Moss, Brendan C. \(GOV\)](#); [Finlaw, Sarah \(GOV\)](#); [Garrity, Rob \(DOT\)](#)
Subject: Re: deadline at noon today —Herald story on Facial Recognition
Date: Friday, June 7, 2019 10:48:03 AM

I am good with them. Thank you.

Sent from my iPhone

On Jun 7, 2019, at 10:35 AM, Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us> wrote:

Hi David,

Do you have any comments on the RMV's draft responses below?

Questions for RMV to answer:

I'm assuming the RMV makes these photos available to police if they ask for it?

The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.

Are there any steps the RMV takes to protect the privacy of individuals?

The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)

Also, besides the RMV, does the DOT use facial recognition in any way?

MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal driver privacy protection act and policy guidelines.

Thanks,

Judi

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Sent: Friday, June 7, 2019 10:12 AM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Cc: Moss, Brendan C. (GOV) <Brendan.C.Moss@MassMail.State.MA.US>; Finlaw, Sarah (GOV) <sarah.finlaw@state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Garrity, Rob (DOT) <rob.garrity@state.ma.us>;

Huber, Maxwell (DOT) <Maxwell.Huber@dot.state.ma.us>; McGlinchey, Madison (DOT) <Madison.McGlinchey@dot.state.ma.us>

Subject: Re: deadline at noon today ---Herald story on Facial Recognition

Thank you

Sent from my iPhone

On Jun 7, 2019, at 9:43 AM, Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us> wrote:

David and Brendan,
Re: Herald questions on facial recognition use.
Please see below for the RMV suggested edits to David's draft comment and in red font RMV answers to RMV questions.

Boston Herald needs comment by noon.

Thanks,
Jacque

DRAFT at 9:45 a.m.

Questions for RMV to answer:

Q: I'm assuming the RMV makes these photos available to police if they ask for it? **The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.**

Q: Are there any steps the RMV takes to protect the privacy of individuals? **The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)**

Q: Also, besides the RMV, does the DOT use facial recognition in any way? **MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal driver privacy protection act and policy guidelines.**

2) Any RMV comments to David Procopio statement?. RMV suggested edits in yellow highlights.

The Massachusetts State Police utilize **(might change utilize to may access)** facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center

as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected **driver's license and identity** fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit (**suggest changing to hit to potential match, not hit**) in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

From: Procopio, David (POL)
<david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT)
<Jacquelyn.Goddard@dot.state.ma.us>;
Marvin, Patrick (DOT)
<Patrick.Marvin@dot.state.ma.us>; Lavoie,
Sara (DOT) <Sara.Lavoie@dot.state.ma.us>;
Riley, Judith (DOT)
<JudithReardon.Riley@dot.state.ma.us>
Subject: Draft response to Herald Re: Facial
Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.
Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our

Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants

involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding

an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone

From: [Riley, Judith \(DOT\)](#)
To: [Procopio, David \(POL\)](#)
Cc: [Moss, Brendan C. \(GOV\)](#); [Finlaw, Sarah \(GOV\)](#); [Garrity, Rob \(DOT\)](#)
Subject: RE: deadline at noon today —Herald story on Facial Recognition
Date: Friday, June 7, 2019 10:50:00 AM

Thank you very much.

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Sent: Friday, June 7, 2019 10:48 AM
To: Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>
Cc: Moss, Brendan C. (GOV) <Brendan.C.Moss@MassMail.State.MA.US>; Finlaw, Sarah (GOV) <sarah.finlaw@state.ma.us>; Garrity, Rob (DOT) <rob.garrity@state.ma.us>
Subject: Re: deadline at noon today —Herald story on Facial Recognition

I am good with them. Thank you.

Sent from my iPhone

On Jun 7, 2019, at 10:35 AM, Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us> wrote:

Hi David,

Do you have any comments on the RMV's draft responses below?

Questions for RMV to answer:

I'm assuming the RMV makes these photos available to police if they ask for it?

The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.

Are there any steps the RMV takes to protect the privacy of individuals?

The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)

Also, besides the RMV, does the DOT use facial recognition in any way?

MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal driver privacy protection act and policy guidelines.

Thanks,

Judi

From: Procopio, David (POL) <david.procopio@pol.state.ma.us>
Sent: Friday, June 7, 2019 10:12 AM
To: Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us>
Cc: Moss, Brendan C. (GOV) <Brendan.C.Moss@MassMail.State.MA.US>; Finlaw, Sarah (GOV) <sarah.finlaw@state.ma.us>; Riley, Judith (DOT) <JudithReardon.Riley@dot.state.ma.us>; Marvin, Patrick (DOT) <Patrick.Marvin@dot.state.ma.us>; Garrity, Rob (DOT) <rob.garrity@state.ma.us>; Huber, Maxwell (DOT) <Maxwell.Huber@dot.state.ma.us>; McGlinchey, Madison (DOT) <Madison.McGlinchey@dot.state.ma.us>
Subject: Re: deadline at noon today --Herald story on Facial Recognition

Thank you

Sent from my iPhone

On Jun 7, 2019, at 9:43 AM, Goddard, Jacquelyn (DOT) <Jacquelyn.Goddard@dot.state.ma.us> wrote:

David and Brendan,
Re: Herald questions on facial recognition use.
Please see below for the RMV suggested edits to David's draft comment and in red font RMV answers to RMV questions.

Boston Herald needs comment by noon.

Thanks,
Jacque

DRAFT at 9:45 a.m.

Questions for RMV to answer:

Q: I'm assuming the RMV makes these photos available to police if they ask for it? **The RMV makes digitized images of credential holders available to law enforcement so law enforcement may confirm the veracity of the credentials presented to them.**

Q: Are there any steps the RMV takes to protect the privacy of individuals? **The dissemination of RMV held images is strictly controlled by the federal driver privacy protection act. (As an example, the DPPA prohibits the RMV from releasing license image photos to the media.)**

Q: Also, besides the RMV, does the DOT use facial recognition in any way? **MassDOT does not use facial recognition beyond the Registry's use which is strictly controlled by the federal**

driver privacy protection act and policy guidelines.

2) Any RMV comments to David Procopio statement?. RMV suggested edits in yellow highlights.

The Massachusetts State Police utilize (might change utilize to may access) facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected driver's license and identity fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit (suggest changing to hit to potential match, not hit) in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

From: Procopio, David (POL)
<david.procopio@pol.state.ma.us>
Sent: Thursday, June 6, 2019 5:31 PM
To: Goddard, Jacquelyn (DOT)

<Jacquelyn.Goddard@dot.state.ma.us>;

Marvin, Patrick (DOT)

<Patrick.Marvin@dot.state.ma.us>; Lavoie,

Sara (DOT) <Sara.Lavoie@dot.state.ma.us>;

Riley, Judith (DOT)

<JudithReardon.Riley@dot.state.ma.us>

Subject: Draft response to Herald Re: Facial Recognition

Please review the below draft of statement/supplemental info for the Herald re: facial technology. This statement is being reviewed by the public safety comms chain, MSP command, and RMV/DOT officials. Please send any comments back and I will review and synthesize any edits from the three groups.

Dave Procopio

The Massachusetts State Police utilize facial recognition technology, when applicable, to further criminal investigations, primarily our Commonwealth Watch Center as well as through our unit attached to the RMV. It is a valuable tool that can help investigators identify criminals and, by doing so, seek justice for their victims and take offenders off the street before they commit another crime.

The State Police unit at the RMV utilizes the technology to investigate suspected license fraud. At the Watch Center, meanwhile, State Police analysts have the capability to use facial recognition to help identify images of crime suspects at the request of

State Police units or other police agencies. Analysts can compare images of unknown suspects against both the RMV database and open-source social media.

It is important to note that a facial recognition hit in and of itself is not a positive identification. Rather, it is an investigative lead that requires further follow up and vetting by case officers. This is part of the training our personnel receive, and when the Watch Center (part of our Fusion Center) performs a facial recognition search for an outside agency, the following disclaimer is provided with the results: *The result of a face recognition search is provided by the CFC only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation.*

As with any other investigative process or technology, use of facial recognition software may only be used for legitimate and clearly defined law enforcement purposes, per MSP general investigative policies.

Several recent examples of leads generated by MSP analysts through facial recognition are below.

Facial Recognition Examples:

I-93 Public Safety Threat – Dirt Bike/ATV Operators

- In February 2018, State Police Analysts assigned to the Commonwealth Watch Center worked with Troopers out of the

Cyber Crimes Unit to identify unknown parties involved in an incident that occurred on I-93 on Saturday, February 24, wherein more than twenty individuals created a traffic situation and public safety threat by operating dirt bikes, ATVs, and other off-road vehicles on the expressway. State Police made seven arrests on scene but many participants remained unidentified. Utilizing open source investigative tools and Facial Recognition on videos and still photographs posted to social media from the event, State Police Analysts were able to identify a number of additional participants involved in the incident.

Armed Robbery, Framingham, MA – Social Media IDs

- In January, the Framingham Police Department requested assistance in identifying four individuals believed to be involved in an armed robbery that occurred on January 14, 2019. Framingham PD was able to provide the web addresses for social media profiles of the four suspects. Through a combination of Facial Recognition and open source exploitation, State Police Analysts assigned to the Commonwealth Fusion Center were able to positively ID the suspects, despite several of them utilizing false names and not possessing Massachusetts Licenses or IDs. All four individuals have active warrants from various police departments, including several for other armed robberies.

Road Rage Incident in Medford

- In January, the Commonwealth Fusion Center was contacted by the Massachusetts

State Police Medford Barracks regarding a road rage incident that occurred at Wellington Circle. The Trooper on scene provided cell phone video of the incident taken from inside the victim's vehicle, depicting an unknown subject approaching and striking the vehicle. Facial Recognition conducted on a still photograph from the video returned a possible match to a Massachusetts Driver's License or ID, which was provided within minutes to the investigator for follow-up.

MSP Crime Gun Unit – Social Media IDs of Gang Members

- In February, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Crime Gun Unit regarding an attempt to identify a series of individuals on social media via Facial Recognition. The individuals, believed to be affiliated with a gang related crimes, were identified through a combination of Facial Recognition and open source exploitation of publicly available information found on social media. In total, the identities of approximately 23 previously unidentified individuals were either confirmed via photograph/tattoo comparison, or tentatively identified via name, date of birth, and geographic profile combined with information publicly available on their profiles.

Gang Identified for Out of State Agency

- In March, the Commonwealth Fusion Center was contacted by the the Criminal Intelligence Center from another eastern state regarding an attempt to identify four members of a street gang believed to have

ties to Massachusetts through publicly accessible social media sources. Through a combination of Facial Recognition and open source investigation, all four suspects were positively identified and their information shared with State Police in the state from which the request originated pursuant to an ongoing investigation.

MSP H-2 Identified Suspect with Felony Warrant(s)

- Also in March, the Commonwealth Fusion Center was contacted by the Massachusetts State Police Framingham Barracks regarding an attempt to identify person suspected of concealing his true identity from police. Facial Recognition on a photograph taken by the investigating MSP Trooper on scene returned a possible match candidate. Subsequent investigation of the suspect corroborated the identification of Name/DOB, and also identified an existing felony warrant under the suspect's true name, resulting in the suspect's arrest.

Sent from my iPhone