Mobile Finger Print – Pilot Report

Program:  Integrated Criminal Justice (ICJ)
Initiative:  Field Based Positive Identification

Version 1.20

Prepared by:

Brian Mouty
Mayor’s Office / Safety
Consultant

Date:

February 10, 2015
Table of Contents

1. Project Description ........................................................................................................ 3
   1.1. Background ........................................................................................................... 3
   1.2. Solutions Installed ............................................................................................... 3
2. Pilot Results ................................................................................................................ 4
   2.1. Pilot Objectives / Results ................................................................................... 4
   2.2. Operational Policy ............................................................................................... 4
   2.3. Officer Feedback .................................................................................................. 4
3. Conclusion ................................................................................................................... 6
   3.1. Appendix A ........................................................................................................... 7
   3.2. Appendix B ........................................................................................................... 10

Revision History

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>Reason For Changes</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brian Mouty</td>
<td>02/10/15</td>
<td>Original Document</td>
<td>1.20</td>
</tr>
</tbody>
</table>
1. Project Description

1.1. Background

In the current business environment, officers are unable to obtain a positive identification of any person contacted in the field. This lack of identification leads to cases filed with the wrong name, missed warrants, and taking misidentified people into custody on warrant arrests. This results in added labor to the criminal justice agencies to correct the error.

This pilot will identify potential solutions to provide positive identification of contacted persons in the field utilizing a high speed data cellular network.

Two vendors provided prototype solutions to demonstrate the feasibility of the solution. The pilot effort ran from 9/1/2014 to 12/31/2014.

The pilot effort assisted DPD with identifying requirements, proving concept feasibility and helping prepare for future solicitation.

1.2. Solutions Installed

For the purposes of this pilot, two vendor solutions were installed, Dynamic Imaging’s Picture Link and MorphTrak’s MorphIdent solution.

Dynamic Imaging - Picture Link

Picture Link by Dynamic Imaging is the current production solution installed at the City and County of Denver to capture fingerprints on all in-custody defendants. Eight units (readers and software licenses) were purchased a few years ago to demonstrate mobile fingerprint identification. However, these units were never installed.

The Executive Director’s Office of Safety worked with the vendor and the City’s Tech Services team to install this solution for use in the pilot.

MorphTrak - MorphIdent

The MorphIdent product is designed to work in conjunction with the MDT or laptop computer that is installed within a police vehicle. The successful use of the MorphIdent device will require that the MDT have access to a specific AFIS server located at the CBI data center in Lakewood.

There is a small application which was installed on the laptop PC.

The MorphIdent hand held device connects to the MDT/laptop in the police vehicle using either a USB cable or Bluetooth. The hand held device is used to capture a person’s prints. The hand held device will then automatically transmit the captured prints to the laptop. The MorphIdent software on the laptop will collect and manage the print submissions and automatically forward them to the State’s AFIS for processing.

Once the matching results have been completed (30 to 60 seconds) the results are returned to the MorphIdent software on MDT/Laptop in the police vehicle. The results can then be reviewed by the officer.
2. Pilot Results

The Pilot was executed in the Gang Unit which was comprised of 19 street officers. This unit was small enough to allow training to all officers and still ensure the IMU could provide technical support as needed.

2.1. Pilot Objectives / Results

<table>
<thead>
<tr>
<th>Objective</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leverage the high-speed cellular data network</td>
<td>Both solutions leverages the new high-speed cellular network successfully.</td>
</tr>
<tr>
<td>Prove that timely finger print capture and response is possible</td>
<td>Both solutions provided timely mobile fingerprint identification.</td>
</tr>
<tr>
<td>Obtain feedback from officers</td>
<td>See Section 2.2</td>
</tr>
<tr>
<td>Identification accuracy rate of 99%</td>
<td>No fingerprint hits were erroneous during the pilot.</td>
</tr>
<tr>
<td>Identification response to officer within 2 minutes</td>
<td>Both solutions provided responses in less than 2 minute.</td>
</tr>
<tr>
<td>Ease of use for officer</td>
<td>Officers were able to successfully use both solutions with less than 1 hour of training.</td>
</tr>
<tr>
<td>Query local, state and federal fingerprint databases</td>
<td>Picture Link solution queried the local City and County of Denver database only. Morpholdent queried the State CBI database and the Federal RISC database. The State database included all the City records as well.</td>
</tr>
</tbody>
</table>

2.2. Operational Policy

As part of this project, DPD created an operational policy on the use of the mobile fingerprint readers. This policy was drafted to ensure appropriate use of the new technology.

A copy of the policy is included in Appendix A.

2.3. Officer Feedback

Below are several real case highlights on usage.

- A park is directly behind the residence where officers contacted three Park Hill Bloods: Suspect A 09-14-94, Suspect B 11-11-89, and Suspect C 08-15-96. Suspect A attempted to use his twin brother’s name. Officers used the fingerprint technology that immediately identified his true identity. He had two outstanding misdemeanor warrants.

- 2300 Hours, Quitman and Tennessee, Officers stopped Suspect A and Suspect B gang member. Suspect B lied about his name, but was identified by the fingerprint reader as having a felony trespass warrant.
• 2040 Hours, Officers stopped Suspect A, he did not have good ID, so was fingerprinted on the reader, which confirmed his identity. He was wanted on two Denver warrants for harassment and traffic, and arrested.

• 1900 Hours, 3100 Lafayette St, Officers jumped an occupied local steal. Three parties ran from the car, but were quickly apprehended. Suspect A gave false info, was cited and taken to the FCC. Suspect B, was arrested for motor vehicle theft, he lied about his identity, but officers used the finger print reader to positively identify him. Suspect B was featured in a wanted bulletin on the roll call clipboard tonight, he had three misdemeanor warrants and a felony probation violation. Suspect C, was wanted on a three warrants and was processed through juvenile intake. Order-ins were completed for the auto theft and sent to D5.

• 1930 Hours, I-70 and Central Park Dr, Officers covered D2 and Aurora PD on a carjacking arrest. They used the new fingerprint scanner to ID Suspect A on scene, the suspect, claimed not to speak English. After taking his finger print and identifying him, he switched to speaking perfect English. Suspect A was arrested for failing to register as a sex offender. Suspect B was arrested for carjacking.

Lt. John Pettinger and Brian Mouty met with the officers in the Gang Unit on 9/30/2014 to obtain some verbal feedback from the usage during the first month. Here are some of the comments that were made.

• Must be able to obtain a fingerprint while the defendant is in handcuffs. Tablets may not be feasible for this.
• The Morpho system is unreliable. CBI replied to this issue stating that the FBI had system issues during August. This only affected Federal queries, not State queries.
• Both systems provided response in less than 30 seconds
• Morpho system was more effective since several contacts were made with defendants from other jurisdictions (i.e. Aurora). They would much rather prefer a search a statewide fingerprint database to only a city wide database.
• The Picture Link solution had a tethered fingerprint reader while the Morpho solution was wireless. The officers stated that both readers worked fine.
• Officers firmly stated they did not want us to take the readers away from them.

Based on the officer feedback, an initial list of requirements have been captured. These requirements are listed in Appendix B.
3. Conclusion

The pilot’s effort convincingly demonstrated the feasibility of providing mobile fingerprint identification in the field at the Denver Police Department. All of the original objectives were met and the system was well received by the officers.

One thing the pilot did not demonstrate, nor did we expect it, was to integrate with RMS. This would be part of a larger effort during full production rollout.

Currently, there is only one vendor, MorphoTrak that provides a solution to hit the CBI CICC statewide fingerprint database. This would limit our options during procurement.

The benefits from this solution stretch well beyond the obvious benefits at DPD. The Denver Sheriff’s Department would save thousands of hours in labor from correcting inmate identities after intake. Denver County Courts, the City Attorney’s office, and District Attorney’s office would save labor hours in correcting “John Doe” cases. Detectives would improve their investigations by being able to identify unknown deceased victims earlier.

Possible funding sources include Federal grant funds for law enforcement, the City iFund or the City General Fund.

The largest expense for this project will be related to equipment and software. Approximately 500 units will need to be purchased to install in each of the DPD vehicles. In addition, motorcycle/horse/bicycle officers will need additional equipment to connect them to the cellular/wireless data network.

A possible strategy would be to implement the solution in a phased approach, limiting the number of units installed and the level of integration with RMS for each year. For example, installing the solution at DSD and all DPD district stations in the first year. In future years, build in the RMS integration and deploy in selected district vehicles as the funds allow.
3.1. Appendix A

Department Directive
2014-1

TO: Officers Involved in Mobile Fingerprint Device Pilot Project

FROM: Robert C. White, Chief of Police

DATE: August 29, 2014

SUBJECT: Operational Policy for Use of the Mobile Fingerprint Device

Selected officers will be provided a handheld mobile fingerprint device from one of two vendors during the pilot. The devices being tested are Picture Link, (accesses the City and County records database) and Morpholdent, (accesses the CBI database). The handheld device used by the officer can capture an individual’s fingerprint in the field and provide a rapid positive identification to the officer. The possible identifications will be limited to subjects maintained in the searched database and does not preclude a record from existing in another database. The mobile devices are only an aid to the identification of a person and shall not be used as the sole grounds for establishing probable cause for arrest.

POLICY:

The mobile fingerprint device will only be used by personnel who have received training in the proper use of the equipment and are part of the pilot.

Officers are reminded that fingerprinting is generally considered part of the “booking process” and officers will not be taking fingerprints, without the individual’s consent, unless there is probable cause to arrest. Officers will not take an individual’s fingerprint on a consensual contact or a reasonable suspicion stop, without the subject’s consent. If at any time the subject withdraws the consent, the officer must stop the fingerprint process.

When an officer issues a traffic citation that is not an arresting offense the driver should not be fingerprinted without giving consent. The mobile fingerprint device will not be used on subjects issued a civil marijuana ticket unless the subject consents. The mobile fingerprint device will not be used on juveniles due to the consent issue which would require a parent or guardian.

1. Voluntary Consent: During a lawful reasonable suspicion detention, the mobile fingerprint device may be used in situations where the subject to be fingerprinted gives a knowing and willing voluntary consent to the use of the fingerprint device. The manner in which the consent is given must be documented on the resulting paperwork or in the absence of any GO, street check or summons, on the officer’s log sheet.

   a. The subject may withdraw consent at any time. If the consent is withdrawn, the use of the fingerprint device is NOT AUTHORIZED and its use must stop immediately. The officer may not force or coerce the subject to submit to the fingerprinting.

2. Without Consent: The mobile fingerprint device may be used without the consent of the subject:
a. Upon arrest of the subject;

b. If authorized in the execution of a valid search warrant; or

c. If specifically required by statute or pursuant to court order

AUTHORIZED USE:

1. **An officer must be able to articulate and justify** the authorized and appropriate use of the mobile fingerprint device based on the policy, training, officer experience and assessment of the circumstances. All uses of the mobile fingerprint device must be **documented** (in the GO, citation, US&C, street check or if no other paperwork is generated, on the officer’s log sheet).

2. **Prior to an arrest or during a lawful detention**, the fingerprint device may be used **with the consent** of the subject if the officer has reasonable suspicion:

   a. The suspect to be printed has committed, is committing, or is about to commit a criminal offense and there is a justifiable and reasonable belief the fingerprint scan will establish or nullify the subject’s connection to the criminal offense

   b. The individual to be printed is subject to an arrest warrant and there is justifiable and reasonable belief the fingerprint scan will establish or nullify the subject’s identity in the execution of the warrant

   c. The subject intentionally gave a false or fictitious name, residence address, or date of birth to the officer when cited for a traffic violation or other misdemeanor

   d. The subject is witness to a criminal offense and intentionally gave a false or fictitious name, residence address, or date of birth to the officer

3. **Subsequent to an arrest**, the mobile fingerprint device may be used **without the consent** of the arrested suspect to verify the identity of the suspect to assist the officer in determining the appropriate arrest routing of the suspect, (jail, order-in etc.)

4. **The mobile fingerprint device may be used without the consent of the subject** if a subject’s fingerprints are required in the execution of a valid search warrant, required by statute, or authorized by court order.

   a. Reasonable force may be used to gain the subject’s compliance with the search warrant or court order. An officer shall use the least amount of force needed to execute the search warrant.

5. **Nonstandard Use of the mobile fingerprint device** requires notification and authorization by a command officer. Some examples of such use include:
a. A traffic fatality investigation in which there is no other reasonable means of identifying a victim AND a member of the coroner’s office is on scene and gives approval

b. An unknown dead investigation in which there is no other reasonable means of identifying a victim AND a member of the coroner’s office is on scene and gives approval

c. A homicide investigation in which there is no other reasonable means of identifying a victim AND a member of the coroner’s office is on scene and gives approval

d. An unconscious party

UNAUTHORIZED USE:

1. Not to be used for random or general investigative or intelligence gathering

2. Not to be used on a juvenile or a person that is suspected to be a juvenile

3. Not to be used when issuing a civil marijuana citation

ANY UNAUTHORIZED USE MAY RESULT IN DISCIPLINARY ACTION
### 3.2. Appendix B

**Initial Requirements**

<table>
<thead>
<tr>
<th>ID</th>
<th>TITLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wireless FP Reader</td>
<td>Wireless FP capture device is preferred for mobility and ease of use.</td>
</tr>
<tr>
<td>2</td>
<td>AFIS Compatible</td>
<td>Must be able to verify FP against CBI AFIS database (State).</td>
</tr>
<tr>
<td>3</td>
<td>Picture Link Compatible</td>
<td>Must be able to verify FP against Denver Picture Link database (Local).</td>
</tr>
<tr>
<td>4</td>
<td>FBI Compatible</td>
<td>Able to verify FP against Federal database (Master DB, RISC, etc.)</td>
</tr>
<tr>
<td>5</td>
<td>FP image to RMS</td>
<td>Provide the FP image to RMS for storage on case specific information.</td>
</tr>
<tr>
<td>6</td>
<td>FP data to RMS</td>
<td>Provide data from FP hit to RMS for storage on case specific information.</td>
</tr>
<tr>
<td>7</td>
<td>4G Cellular Network</td>
<td>Able to traverse CCD 4G cellular data network.</td>
</tr>
<tr>
<td>8</td>
<td>Data Radio Network</td>
<td>Able to traverse existing CCD data radio network as backup.</td>
</tr>
<tr>
<td>9</td>
<td>Mug Shot in return data</td>
<td>The photo of the identified individual will be available and displayed to the officer.</td>
</tr>
<tr>
<td>10</td>
<td>Mobile device weather resistant</td>
<td>The mobile FP capture device must be able to function in various weather conditions, including but not limited to: Rain, snow, temps range -20 to 120 degrees.</td>
</tr>
<tr>
<td>11</td>
<td>FP response time</td>
<td>Response time is less than 2 minutes from point of sending valid FP image.</td>
</tr>
<tr>
<td>12</td>
<td>CJIS requirements</td>
<td>Must satisfy all CJIS requirements</td>
</tr>
<tr>
<td>13</td>
<td>Assist in dual authentication CJIS requirement</td>
<td>Utilize FP capture device to perform dual authentication for officer logon to MDT.</td>
</tr>
<tr>
<td>14</td>
<td>WIFI network</td>
<td>Able to traverse Wi-Fi 802.11 a/b/g network when available.</td>
</tr>
<tr>
<td>15</td>
<td>Data Encryption</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Battery life</td>
<td>Mobile unit must be able to run on battery power for at least 10 hours.</td>
</tr>
<tr>
<td>17</td>
<td>Recharge Battery</td>
<td>Mobile fingerprint reader must be able to be recharged in a patrol car and standard 110v outlet.</td>
</tr>
<tr>
<td>18</td>
<td>Interface with NCIC/CCIC</td>
<td>Provide automatic reply to wants/warrants</td>
</tr>
<tr>
<td>19</td>
<td>Multiple FP captures</td>
<td>System capable of capturing fingerprints for up to 5 individuals before submitting prints for processing.</td>
</tr>
<tr>
<td>20</td>
<td>Search for warrants</td>
<td>System capable of automatically searching for warrants without manual data input by officer.</td>
</tr>
<tr>
<td>21</td>
<td>Tablet Compatibility</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Motorcycle Compatibility</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Poor FP Recognition</td>
<td>Ability to recognize if the FP taken is of poor quality. This is important to avoid &quot;not found&quot; results due to a poor FP taken by the officer.</td>
</tr>
<tr>
<td>ID</td>
<td>TITLE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>24</td>
<td>Store FP temporarily</td>
<td>If officer cannot run a successful FP query (i.e. Network down), the system should store up to 5 FP temporarily, so officer can run the prints when the system is available.</td>
</tr>
</tbody>
</table>
| 25 | Mobile Device data presentation | If the mobile FP device is wireless, the Mobile FP device should display the following information after processing a FP.  
- Full Name  
- DOB  
- Photo  
- Dangerous Indicator  
- Warrants Indicator |
| 26 | Mobile Device notifications  | If the mobile FP device is wireless, the Mobile FP device should provide the following notifications after processing a FP.  
+ Audible (able to silence if desired)  
- Positive Hit  
- Not Found  
- Dangerous  
- Warrants  
+ Vibration  
- Positive Hit  
- Not Found |
| 27 | Windows Compatibility       | Application must be able to run on a windows based platform - laptop and tablet.                                                             |
| 28 | DSD Functionality           | Must be able to address DSD requirements. This would include requirements for the Hospital "intake" - MOUTY EXPAND THIS |
| 29 | ID Bureau                   | Must be able to address ID Bureau requirements - MOUTY EXPAND THIS                                                                            |
| 30 | Finger Print Match Confidence Indicator | System will show the level of confidence the algorithm has with the finger print match. (i.e High, Med, Low). This will provide the user the necessary feedback to possibly run the FP again, or do some additional research to confirm the identity. |
| 31 | STATE ID (SID) Capture      | System must capture SID for use as the defendant unique identifier for all criminal justice agencies.                                           |