ICE'S EDDIE PROGRAM:

How ICE Uses Biometric Scanner Tech To Ramp Up Raids

mijente

JUST FUTURES LAW

ABOUT JUST FUTURES LAW

Just Futures Law is a women of color-led immigration lawyering project that works to support the immigrant rights movement in partnership with grassroots organizations. JFL staff have decades of experience in providing technical assistance, written legal resources, litigation, and training for attorneys, advocates, and community groups in various areas of immigration law, particularly at the intersection of criminal and privacy law.

Writer: Paromita Shah

Researchers: Julie Mao and Paromita Shah

Editors: Sejal Zota, Ellen Kemp

Report Layout: Vera Parra

ACKNOWLEDGMENTS

This research project began in 2017 with Julie Mao, Paromita Shah, and Mijente staff. Mijente and Just Futures Law are grateful to the many individuals who helped with this research and expertise. Mijente and Just Futures Law thank Jones Day and the National Immigration Project of the National Lawyers Guild (NIPNLG), particularly Khaled Alrabe, for their legal work on the Freedom of Information Act lawsuit to reveal EDDIE to the public. You can learn more about NIPNLG's work on the suit at https://nipnlg.org. We also thank Trin Mitra for his analysis of FOIA data, Aaron Lackowski for his research on EDDIE contracts, and Katherine Montañez-Montes.

Report Published: November 2020

TABLE OF CONTENTS

I. REPORT BACKGROUND

In 2016, Chicago organizers reported that Immigration and Customs Enforcement (ICE) had arrested several day laborers on the street after using a fingerprint scanning device.[1] Other reports followed - ICE used fingerprint scanners in home raids in New York and vehicle stops in North Carolina. During the raids, people said ICE pressed fingers on fingerprint scanners, took pictures of their faces, and questioned them before being selected for deportation. These reports confirmed our suspicions that the Department of Homeland Security (DHS) was working with a new device for raids and arrests.

This report shares exclusive information acquired from a Freedom of Information of Act (FOIA) lawsuit[2] on mobile handheld devices and an app called "EDDIE" that was created for DHS, including ICE and Customs and Border Patrol (CBP). EDDIE collects and shares – *in real time*- fingerprints, facial scans, location information, and immigration history during immigration raids.[3]

EDDIE is a key component of DHS's militarized biometric collection enterprise that feeds into vast, secretive databases.[4] The overall plan for biometrics is to capture, store, and share with other law enforcement agencies our DNA, iris scans, facial scans, palm prints, voiceprints, gaits, and, of course, fingerprints. EDDIE biometric scans ramp up deportations and incarceration for Black and Brown communities, including immigrant communities.

Conceived and launched during the Obama administration, EDDIE found widespread support within DHS. The Trump administration centralized carceral technologies like EDDIE, into its ICE and CBP enforcement strategy that spills into dozens of other countries. For example, DHS uses an international EDDIE-counterpart called BITMAP (Biometric Identification Transnational Migration Alert Program) against thousands of migrants, including children.

The FOIA documents revealed that the private corporations behind EDDIE have created a suite of surveillance technologies from our bodies - iris, palm, vein, voice, and facial recognition. Research of Privacy Impact Assessments (PIAs) and regulations demonstrated EDDIE's integration into ICE's targeting.

ICE contracts with companies like NEC and Palantir are fueling the meteoric rise of a new tech sub-agency within DHS, the Office of Biometric Identity Management (OBIM), which holds and "analyzes" biometric data. As biometric data collection and analysis assumes a more central role in ICE's portfolio of tech policing, we expect that more and more ICE agents will interrogate people in the field where abuse is most likely to occur but hardest to stop. Privacy protections are not sufficient to protect against profiling and abuse. The Biden administration has a golden opportunity to fix what it started and move away from the development and deployment of carceral, militarized technologies. The incoming President's commitment to criminal justice and immigration reform must include a commitment to cut the use and funding of these technologies before they do more harm.

II. EXECUTIVE SUMMARY

- **EDDIE is much more than mobile fingerprinting.** ICE pairs mobile fingerprinting technologies, including EDDIE, with location tracking, facial scan technologies, and iris scans. Nearly 100% of biometric captures include location services. ICE also stores this biographic information. ICE planned to expand EDDIE into iris and facial recognition.
- **EDDIE transactions are fast and hit many databases at once.** Once ICE captures a fingerprint, queries of federal databases take less than a minute. EDDIE sends transactions to the FBI's Next Generation Identification system, Department of Defense databases, and multiple DHS databases, including IDENT and **Homeland Advanced Recognition Technology (HART)** that will include physical characteristics, biometric, biographic, encounter information, and other personal information about millions of citizens and non-citizens.
- **ICE Homeland Security Investigations (HSI) and Enforcement Removal Officers (ERO) Fugitive Operations Teams are the primary users** of mobile fingerprinting – domestically *and* internationally. The international counterpart of EDDIE is BITMAP.
- **The FOIA results expose that ICE emphasizes using EDDIE on "collaterals."** ICE claims to go after targets using EDDIE, but 55% of fingerprint captures ended up in a match. This means that when ICE used EDDIE to collect fingerprints and photos, only half of the people had an immigration or criminal history. Moreover, FOIA documents show ICE officials expect to stop, detain, and arrest 'collaterals' in EDDIE raids.
- **Documents show that Alternatives to Detention (ATD) teams use EDDIE.** ICE administers the ATD program with contractor assistance using case management and electronic monitoring to ensure people comply with release conditions.
- **EDDIE was deployed in all ICE Areas of Responsibility (AORs)**. Every ICE Field Office across the U.S. used EDDIE with supporting biometric collection tech.
- **Mobile fingerprinting using EDDIE and other tech is already used on children and adults.**
- **ICE only tracked and monitored how much EDDIE was being used, and not whether agents violated rights when they used it. There are serious legal concerns beyond privacy rights** because of the way that agents use this technology to target anyone who they believe is a noncitizen.

III. INTRODUCTION TO EDDIE

EAGLE Directed Identification Environment (EDDIE) is a mobile application that allows ICE to capture a person's fingerprints and face and run remote identification checks against biometric databases during on-site ICE field operations. In operation since 2015, ICE claims EDDIE's main benefit is "instantaneous" feedback without the need to carry around bulky equipment. This means ICE can use it in any raid, any check-in, or in any vetting process of a person who the agency believes is a noncitizen. DHS developed EDDIE in response to a 2014 Appropriations package to "upgrade biometric data collection and analysis technology" for fugitive operations teams, the team most involved in making ICE arrests.[5]

ICE marketed EDDIE as a concrete step in next-gen policing that would exponentially increase deportations. An agent in Little Rock, Arkansas explained how EDDIE fingerprinting was designed to work on the "streets" and "greatly increase the effectiveness of officers."[6]

ICE Correspondence describing EDDIE in a local ICE Field Office, see ICE FOIA 2018-ICLI-00008, P2303

Sent: Tuesday, July 25, 2017 10:01 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: Eddie Scanners

The Eddie scanners are portable biometric data collection and comparison devices that greatly increase the effectiveness of officers. They allow an officer that is "Out in the field" the ability to quickly identify a person based on their fingerprints. This device can be used when screening large groups, as in a detention center, or small groups of individuals encountered "On the street". In conjunction with our service issued iphones, the device is connected to the Service data base which quickly reveals any identification information, criminal history, and immigration history associated with the submitted fingerprints. Having this information readily available at the time of an encounter, a decision can be quickly made to determine detainability/removability in a safe manner.

(b)(7)(E)

Under the new administration and corresponding executive orders, more subjects are now amenable to removal. All available officers are now directed to target these "At-large" subjects with much greater frequency. Every officer does not need an assigned Eddie device, but a supply of Eddie devices needs to be readily available for use on a daily basis, as needed. These devices can be assigned to, and controlled by, the SDDOs at their respective offices for issuance to their officers dependent on the officer's daily assignment.

(b)(6);(b)(7)(C)
Assistant Field Office Director
Department of Homeland Security
Immigration and Customs Enforcement
Enforcement and Removal Operations
Little Rock, Arkansas
(501) 370-(b)(6); - office

IV. HOW DOES EDDIE WORK?

EDDIE is downloaded from the ICE App Store on ICE-issued smartphones. EDDIE captures fingerprints, facial scans, location information, and additional text-based biographic information.[7] It connects with **EAGLE** (EID Arrest Graphical User Interface (GUI)), a booking application used by ICE to process information from individuals.[8] EAGLE is connected to several DHS databases.

An EDDIE "transaction" begins when an ICE officer encounters or targets any person who they believe is a noncitizen whom they want to interrogate. Using a fingerprint scanner, the ICE agent takes fingerprints from the individual which are then uploaded to an iPhone or iPad.

Picture from inSight article on EDDIE and NeoScan, August 30, 2017, from ICE FOIA documents.[9]

After EDDIE authorizes the officer using it, the agent takes a photo of the person while the phone collects location information. ICE claims it stores photographs for 30 days unless the subject is "booked."

Photo of ICE agents using mobile fingerprinting tech in CNN's "Undercover in a "Sanctuary City", a ride-along with ICE in Chicago. Chicago has several "sanctuary city" policies.

After ingesting the fingerprints, EDDIE searches multiple biometric federal databases (Department of Homeland Security, FBI, US Marshals, Department of Defense), and returns results (Hit/No Hit/Error) in less than a minute.[10] Results include any encounters the person has had with DHS and a "rapsheet." The app also allows the agent to insert biographic information about the person. All of these transactions occur within EDDIE.

Picture from inSight article on EDDIE and NeoScan, August 30, 2017[11]

All biometric information collected by EID will be stored in OBIM, where analysts will review biometric information, assess it, and share their interpretations of the data with ICE agents.[12] An ICE agent or a DHS analyst consulted by an ICE agent compares the photos and fingerprints with information they have in their systems. (See Appendix A for a process schematic.)

As the pictures show, DHS aimed to use EDDIE as a way to conduct raids and bypass booking procedures in a police station. Under EDDIE, ICE agents do not ask for consent to take photos or fingerprints. A decision to arrest someone is often made *after* the fingerprints and photos are taken. These components of mobile biometrics raise serious concerns about racial profiling, abuse, and intrusive biometric collection without any recourse or accountability.

V. WHAT IS THE TECH BEHIND EDDIE?

EDDIE is an app integrated with face scan technologies, location information, fingerprint readers, and biographic collection. Multiple agencies within ICE are involved in EDDIE's implementation and deployment, including a significant number of contractors and corporations.[13] These contractors assisted with the development of mobile fingerprinting technology, installation, privacy reviews, analysis, procurement, and maintenance of all EDDIE-related devices.

Picture of NeoScan 45 device from NEC.com: The unit uses LED indicators to guide fingerprint capture. Fingerprints are taken one or two fingers at a time.

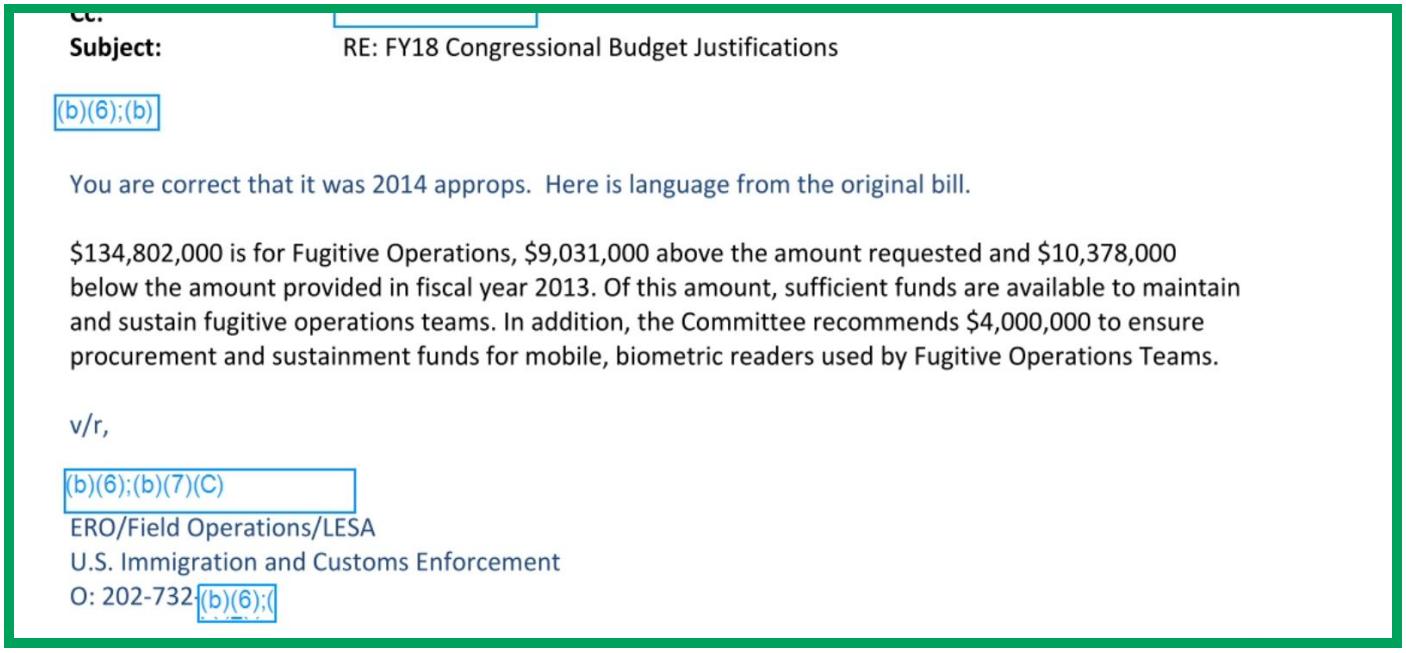
One such contractor was NEC Corporation, which developed the highly-portable NeoScan 45 device to scan fingerprints and to work specifically with the EDDIE app. NeoScan is compatible with Apple iOS and Android operating systems, and it connects via Bluetooth or Wi-Fi.[14]

In 2015, ICE had acquired about 800 NeoScan devices.[15] ICE recommended that each Fugitive Operations team working in the field share at least two devices. At times, individual ICE Field Offices requested additional devices from ICE Headquarters. EDDIE and the NeoScan collect biographic *and* biometric information. NeoScan is powered to do 200 scans before needing another charge. NeoScan devices did not perform facial recognition, but DHS planned for EDDIE to incorporate facial and iris recognition.

VI. HOW MUCH DID EDDIE COST?

While the EDDIE app itself cost about $180,000, millions were needed to integrate, deploy, and support EDDIE in the field.[16] A review of contracts shows that it is estimated that ICE has spent an estimated $46 million dollars on mobile fingerprinting devices, maintenance, and analytical support since 2012. Each NeoScan-45 scanner costs approximately $2,300 per unit, with maintenance costs of approximately $350 per unit per year.[17]

Overall, yearly congressional funding for biometrics was difficult to identify because Congress rarely identifies specific technologies in federal spending bills. But in one instance, Congress allocated funds for fugitive operations teams (FOT) in the 2014 Appropriations package. Of those funds, ICE designated $4 million for NeoScan devices and related technologies and services.[18]



Subject: RE: FY18 Congressional Budget Justifications

(b)(6);(b)

You are correct that it was 2014 approps. Here is language from the original bill.

$134,802,000 is for Fugitive Operations, $9,031,000 above the amount requested and $10,378,000 below the amount provided in fiscal year 2013. Of this amount, sufficient funds are available to maintain and sustain fugitive operations teams. In addition, the Committee recommends $4,000,000 to ensure procurement and sustainment funds for mobile, biometric readers used by Fugitive Operations Teams.

v/r,

(b)(6);(b)(7)(C)
ERO/Field Operations/LESA
U.S. Immigration and Customs Enforcement
O: 202-732-(b)(6);(

ICE Agent describes funding sources for mobile fingerprinting, specifically NeoScan-45

VII. KEY CONTRACTORS BEHIND EDDIE

Key contractors associated with the development and evaluation of the EDDIE application include:

- **NEC Corporation (www.nec.com):** NeoScan was designed by NEC, a worldwide leader in identity technology, analytical products, and service.[19] Based in Japan, NEC is building a vast platform of biometric products for the world - such as face scanners, drones, no-contact iris scans, and gait walking. Services include big data analytics, cloud services, and biometric authentication. Most of their products are designed for law enforcement, military, security, and immigration agencies, including ICE and CBP. NEC recently invested $1 billion dollars into India's identity market, with a special focus on Aadhar – the largest biometric identity card experiment in the world. NEC sells its products through NEC Corporation of America, Wexler Technical Solutions, and Government Acquisitions Inc.

- **Booz Allen Hamilton (www.boozallen.com)**: Booz Allen Hamilton is one of the largest government contractors in the world. Booz Allen contractors are deeply embedded within ICE. They work with multiple offices associated with EDDIE, including, but not limited to, the ICE Privacy and Records Office, Information Governance and Privacy Office, and the Mobile Working Group developing use cases, features, and requirements for EDDIE. They make recommendations around compliance with privacy rules and regulations and procurements.

- **Government Acquisitions Inc. (www.gov-acq.com)**: Government Acquisitions Inc. (GAI) is a small business contractor that served as the NEC Corporation reseller for the NeoScan 45 finger scanning devices. For about 800 devices, GAI earned $2 million.[20] GAI President Jay Lambke said the devices would be key to helping ICE "leverage the rapid capture of biometrics by officers and agents in the field.[21]

- **Dev Technology Group (www.devtechnology.com):** Dev Technology is a contractor involved with database interoperability and data analysis. They have been awarded hundreds of millions of dollars in their contracts with ICE, CBP, Transportation Security Agency (TSA), and DOD. They continue to develop or support biometric applications for DHS. Between FY2014 and 2018, ICE reserved $83 million for Dev Technology group. Work related to EDDIE and EID is estimated at $6M.[22]

- **Wexler Technical Solutions (www.wtscomputing.com):** Wexler Technical Solutions (WTS) has provided information and guidance on how systems store and capture fingerprint data and developed the EDDIE application. They are credited with developing the EDDIE app itself. Between FY2014 and 2018, ICE obligated near $38 million to WTS. Marc Wexler, President of WTS, said, "The Eagle Direct Identification Environment mobile biometrics app allows agents to fingerprint detainees and connect to their databases faster and is 'helping us catch bad guys.'"[23]

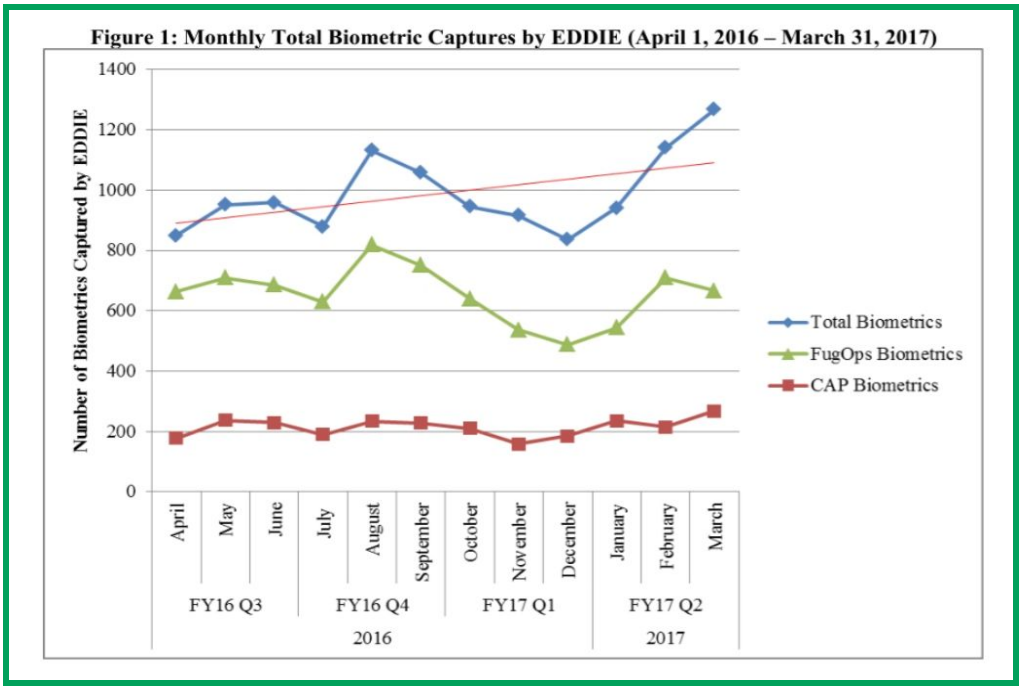
VIII. WHICH DHS AGENCIES USE EDDIE?

In June 2017, ICE had trained about 2,000 officers to use EDDIE.[24] In 2015, DHS purchased 800 EDDIE scanners. But after President Trump was elected, officers wrote that they were "inundated" with requests.[25]

- **ICE Homeland Security Investigations (HSI)** - HSI, the criminal investigative arm of ICE, has long been subject to investigations of abusive tactics and lack of oversight. They operate domestically and internationally. HSI and Mexican immigration officers also use EDDIE to identify Mexican migrants entering the United States.[26]

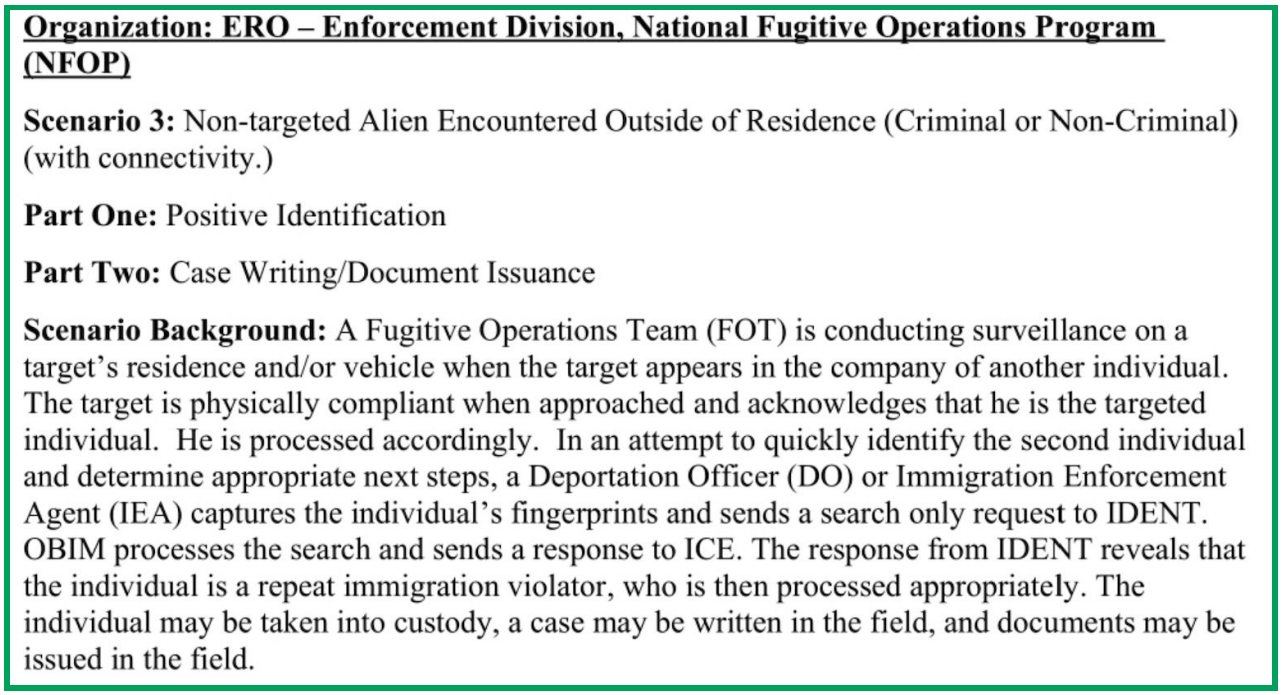
Picture from FOIA documents HSI program document on EDDIE (on file with author)

- **ICE Enforcement and Removal Operations (ERO)** - ERO oversees programs related to detention and deportation of noncitizens, and includes the Criminal Alien Program (CAP), Fugitive Operations (FugOps), and Alternatives to Detention. Fugitive Operations teams conduct most raids. ERO data from the FOIA suit shows that 90% of usage comes from ERO, with about 90% of that use from FugOps Team.[27]



A chart showing the total number of fingerprints taken by ICE agents in 2016 and 2017 (see endnote 27)

- **DHS Office of Biometric Identity Management (OBIM)** "provides biometric match, store, share, and analyze services to DHS and mission partners."[28] OBIM analysts review fingerprint results and other inputs through EDDIE. They are the analysts within DHS and will review, assess, and potentially determine outcomes of biometric data collected by DHS. Located within DHS' Management Directorate, it is one of the fastest-growing sub-agencies within DHS, currently funded at over $200M. (OBIM is the successor to US-VISIT, a long-standing DHS program analyzing visitor and immigrant information.)



Organization: ERO – Enforcement Division, National Fugitive Operations Program (NFOP)

Scenario 3: Non-targeted Alien Encountered Outside of Residence (Criminal or Non-Criminal) (with connectivity.)

Part One: Positive Identification

Part Two: Case Writing/Document Issuance

Scenario Background: A Fugitive Operations Team (FOT) is conducting surveillance on a target's residence and/or vehicle when the target appears in the company of another individual. The target is physically compliant when approached and acknowledges that he is the targeted individual. He is processed accordingly. In an attempt to quickly identify the second individual and determine appropriate next steps, a Deportation Officer (DO) or Immigration Enforcement Agent (IEA) captures the individual's fingerprints and sends a search only request to IDENT. OBIM processes the search and sends a response to ICE. The response from IDENT reveals that the individual is a repeat immigration violator, who is then processed appropriately. The individual may be taken into custody, a case may be written in the field, and documents may be issued in the field.

Snapshot of scenario planning for EDDIE use by Fug Ops and OBIM, ICE FOIA 2018-ICLI-00008, P. 3667

IX. FEDERAL DATABASES SEARCHED BY EDDIE

Dozens of federal and regional databases that federal law enforcement use are queried by ICE through EDDIE and EAGLE, including DHS, the Federal Bureau of Investigation, and the Department of Defense. EDDIE populates multiple databases with biometric and biographic information.

- **DHS's Automated Biometric Identification System (IDENT) and HART**

  IDENT is a DHS-wide system for the storage and processing of biometric and limited biographic information for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions. IDENT is also used for testing, training, management reporting, planning and analysis, and other administrative uses. Since its launch in 1994, IDENT now contains 230 million unique identities.

  ICE is presently migrating IDENT to HART (Homeland Advanced Recognition Technology), a new massive multi-modal biometric database. HART has greater storage and matching capabilities, particularly for face and iris, voice, DNA, and other biometric modalities. HART also exchanges and shares information with many more government databases.

- **The Enforcement Integrated Database (EID)**

  EID in DHS captures and maintains information related to investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE and CBP.

- **Person Centric Query Service (PCQS)**

  PCQS is a service that allows users to submit a query and view all transactions involving immigrants or non-immigrants across multiple DHS and external systems. It provides a consolidated view of information obtained from an individual's past interactions with DHS such as name, DOB, family relationships, and other personal information.[29]

- **FBI's Next Generation Identification (NGI) System and NCIC**

  NGI is an FBI database. It is the FBI's fully automated national fingerprint identification and criminal history reporting system and is the largest biometric database in the world. Any police officer and DHS officer has access to NGI. EDDIE also feeds into the *Repository of Individuals of Special Concern (RISC)*[30], which is primarily accessed by US Marshals, a large police agency that is heavily involved in the transfers of detained immigrants.

- **Other databases that EDDIE can tap include:**

1. *Automated Biographic Information System (ABIS):* ABIS is the Department of Defense's version of NGI, but is used to identify "national security" threats.

2. *Benefit Biometric Support System (BBSS)* is a DHS enterprise system designed to transmit demographic and fingerprint/biometric data collected at the USCIS Applicant Support Centers (ASCs) for subsequent submission to the FBI.

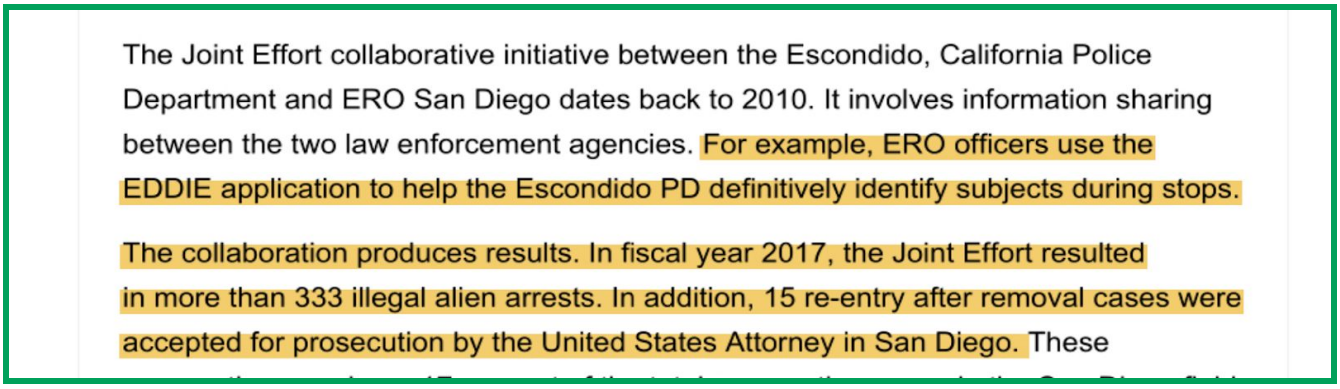
3. *Marriage Fraud Amendment System (MFAS)* is an older case tracking system in DHS designed to identify marriage immigration fraud.

4. *Interpol*: the international police agency between 180 countries.

X. HOW ICE USES EDDIE IN CITIES AND STATES

ICE, EDDIE, AND LOCAL POLICE

ICE has used EDDIE in joint operations with local police. This kind of coordination will allow police to bypass their normal arrest and booking procedures and effectuate an immediate transfer to ICE custody. For example, in 2017, ICE Enforcement and Removal Officers used EDDIE when they worked with the Escondido Police Department to arrest people during traffic stops.



The Joint Effort collaborative initiative between the Escondido, California Police Department and ERO San Diego dates back to 2010. It involves information sharing between the two law enforcement agencies. For example, ERO officers use the EDDIE application to help the Escondido PD definitively identify subjects during stops.

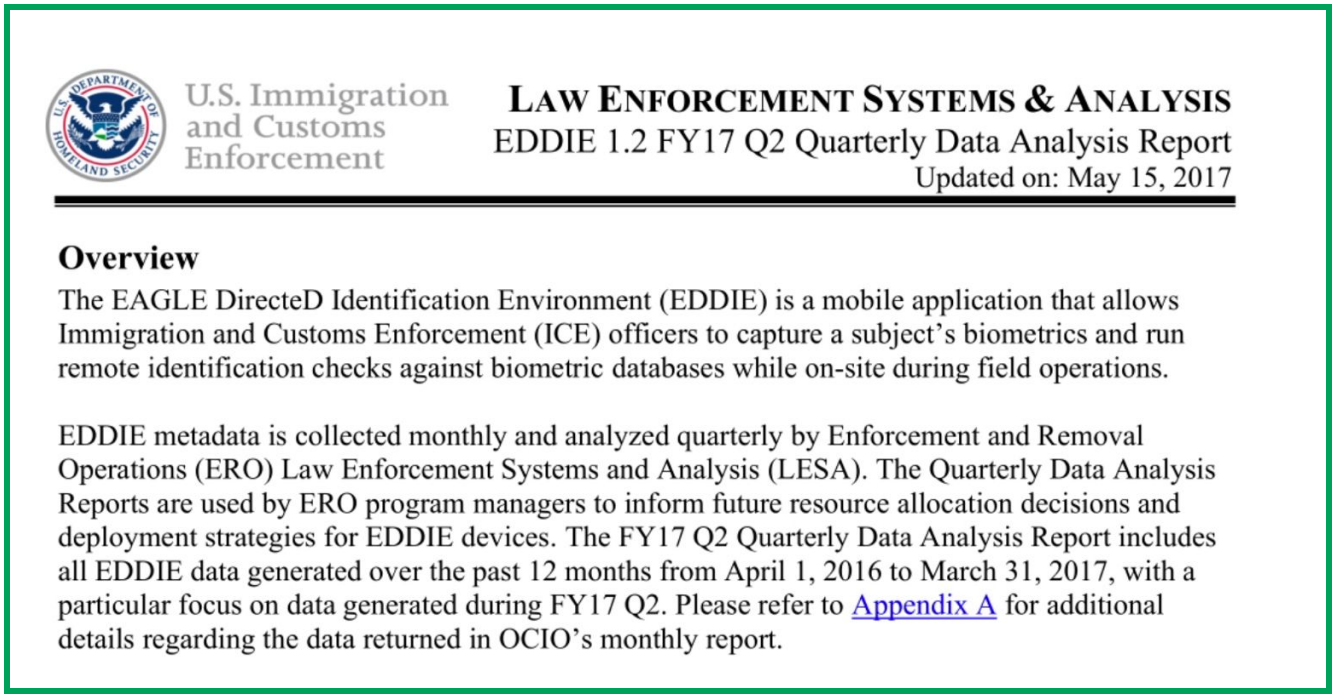
The collaboration produces results. In fiscal year 2017, the Joint Effort resulted in more than 333 illegal alien arrests. In addition, 15 re-entry after removal cases were accepted for prosecution by the United States Attorney in San Diego. These

ICEBreaker, October 16. 2017," ICE FOIA – 2018-ICLI-00008, p240

ICE officers claimed they used EDDIE to help local police screen individuals upon request. This occurred after initial fingerprint checks did not show immigration status.[31]

DATA ON LOCAL USE OF EDDIE

ICE tracked ICE agents' use of EDDIE within their 24 Areas of Responsibility (AOR) through a "Quarterly Data Analysis Report."



U.S. Immigration and Customs Enforcement

LAW ENFORCEMENT SYSTEMS & ANALYSIS

EDDIE 1.2 FY17 Q2 Quarterly Data Analysis Report

Updated on: May 15, 2017

Overview

The EAGLE DirecteD Identification Environment (EDDIE) is a mobile application that allows Immigration and Customs Enforcement (ICE) officers to capture a subject's biometrics and run remote identification checks against biometric databases while on-site during field operations.

EDDIE metadata is collected monthly and analyzed quarterly by Enforcement and Removal Operations (ERO) Law Enforcement Systems and Analysis (LESA). The Quarterly Data Analysis Reports are used by ERO program managers to inform future resource allocation decisions and deployment strategies for EDDIE devices. The FY17 Q2 Quarterly Data Analysis Report includes all EDDIE data generated over the past 12 months from April 1, 2016 to March 31, 2017, with a particular focus on data generated during FY17 Q2. Please refer to Appendix A for additional details regarding the data returned in OCIO's monthly report.

EDDIE 1.2 FY 17 Quarterly Data Analysis Report, May 15, 2017 (ICE FOIA 2018-ICLI-00008, p2128)

Several interesting facts emerged from these documents:

- By May 2017, NGI and IDENT hits hovered around 55%. This means that when ICE used EDDIE to collect fingerprints and photos, only half of the people had an immigration or criminal history. This suggests ICE significantly uses EDDIE against non-targets, i.e. "collateral" arrests.
- By May 2017, most arrests occurred between 4am and 12pm. ICE recommended two NeoScan devices per team.
- By May 2017, nearly all EDDIE transactions provided location information, averaging between 99-100%.

Table 11: Percentage of Biometric Captures by EDDIE with Location Services Enabled

AOR	FY16 Q3 Average	FY16 Q4 Average	FY17 Q1 Average	FY17 Q2 Average
ATL	97.1%	98.8%	100.0%	100.0%
BAL	96.1%	100.0%	100.0%	100.0%
BOS	62.2%	79.4%	72.3%	100.0%
BUF	100.0%	100.0%	100.0%	100.0%
CHI	83.4%	98.2%	95.0%	99.5%
DAL	100.0%	90.3%	96.9%	99.1%
DEN	100.0%	100.0%	59.4%	100.0%
DET	93.3%	100.0%	100.0%	99.4%
ELP	77.8%	100.0%	100.0%	100.0%
HOU	80.0%	100.0%	61.7%	100.0%
LOS	96.1%	95.8%	100.0%	100.0%
MIA	100.0%	100.0%	100.0%	100.0%
NEW	93.1%	95.9%	93.2%	100.0%
NOL	83.8%	81.4%	89.0%	100.0%
NYC	100.0%	100.0%	100.0%	100.0%
PHI	93.0%	85.4%	84.7%	100.0%
PHO	78.6%	54.5%	85.7%	100.0%
SEA	100.0%	100.0%	100.0%	100.0%
SFR	81.4%	89.1%	85.3%	99.1%
SLC	100.0%	100.0%	100.0%	99.6%
SNA	60.0%	66.7%	95.1%	100.0%
SND	100.0%	100.0%	75.0%	100.0%
SPM	100.0%	93.2%	96.7%	100.0%
WAS	46.8%	65.5%	77.1%	100.0%
Total	**89.3%**	**92.2%**	**91.2%**	**99.8%**

Table showing that almost 100% of EDDIE transactions in ICE AORs collect location information, see 2018-ICLI-00008, p2137

From 2015 through 2017, some sanctuary cities saw increasing use of EDDIE. (see Appendix B) This was reinforced in CNN's special *Undercover in a "Sanctuary City"*, where ICE agents discussed the need for these devices because of Chicago's sanctuary city policies and again in Netflix's *Immigration Nation*, Episodes 1 and 3, where arrests occurred in New York City.

XI. EDDIE GOES GLOBAL: THE RISE OF BITMAP

Biometric Identification Transnational Migration Alert Program (BITMAP) is a core program in the Homeland Security Investigations International Operations (HSI-IO), a unit within ICE that trains and equips foreign governments to collect and share biometric and biographic data on migrants outside the United States.[32] It began in 2011 and has since expanded to 14 countries. (HSI-IO operates within 46 countries.) HSI coordinates with embassies and attachés to roll out BITMAP and with CBP, DOD, and the Department of State.[33]

As of February 2020, there were 176,000 people enrolled in BITMAP.[34]

Source: HSI International Components of EDDIE, 2018-ICLI-00008, p 2375

ICE has used BITMAP to collect DNA, photos, and other scans from migrants and their children, including asylum seekers. An *Intercept* article exposed ICE's use of BITMAP information in immigration court. The agency argued that the data was reliable to identify the ages of children.[35] A federal judge, however, ruled that the BITMAP information was poor, and ordered the young people released.[36]

In 2017, ICE removed the age limitations around biometric collection, allowing ICE to take fingerprints, photographs, and DNA from anyone they encountered. This means BITMAP can be used on people outside the United States who want to seek asylum here. More importantly, ICE HSI wanted BITMAP to potentially stop people from making a valid entry.

Rep. McCaul (R-TX) has repeatedly introduced bills, with strong bipartisan support, to expand BITMAP, by amending the Homeland Security Act.[37] Only Rep. Bennie Thompson (MI) raised objections to BITMAP. Congress has not conducted any oversight hearings of the program, and little is known about the interest around this bill, other than to secure funding for this program.

As of late 2016, BITMAP was operating in the Philippines, Panama, Costa Rica, Honduras, Guatemala, El Salvador, Mexico, Dominican Republic, and Colombia. Data gathering is based on the suspicions of foreign law enforcement counterparts. BITMAP checks biometric information against three primary US law enforcement databases – IDENT, NGI, and ABIS and "enrolls" individuals into the program.

BITMAP FLOW AND REQUIREMENTS

For a new country to participate in BITMAP, DHS takes the following steps with the host country. The US Ambassador and HSI attaché support are usually involved.

The following are key steps in the BITMAP process flow:

- Foreign law enforcement collects biometric data
- They share the data with HSI and CBP
- HSI/CBP vets and reviews data
- ICE/HSI searches the data and enrolls it in DoD, FBI, DHS databases
- Match/no match results are delivered to designated DHS and DoD personnel.

CORPORATE CONNECTIONS BETWEEN EDDIE AND BITMAP

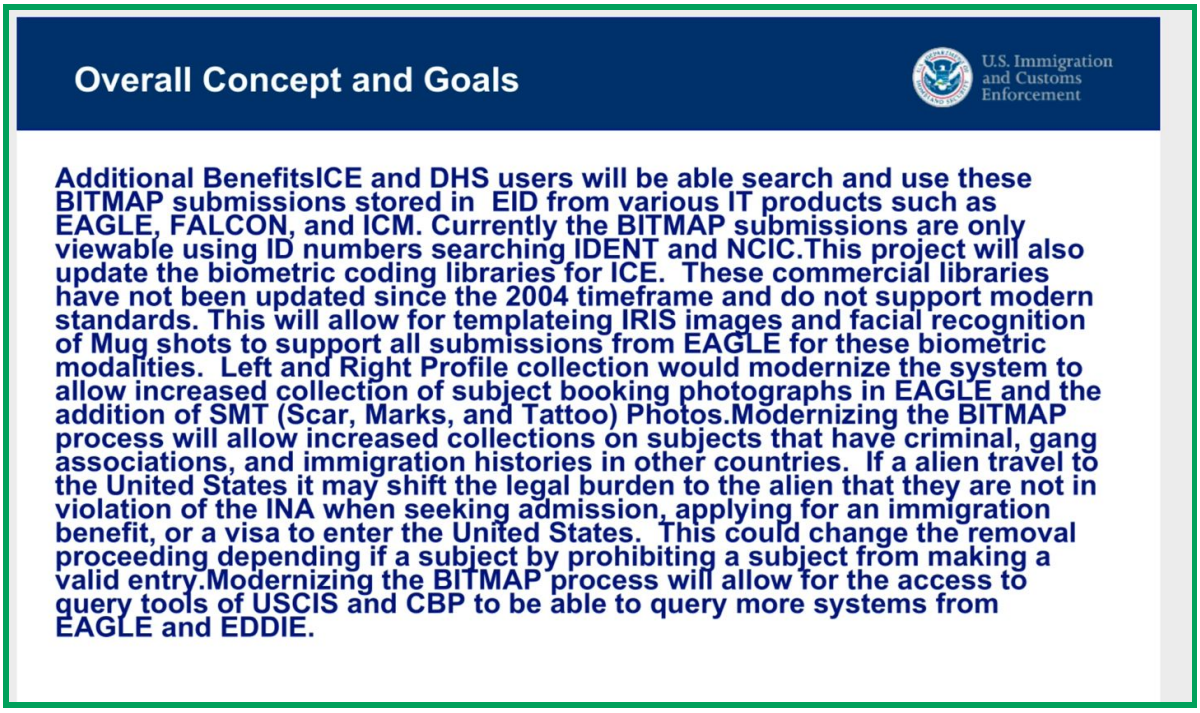
ICE agents viewed EDDIE and BITMAP as complementary tools for enforcement – domestically and internationally.

BITMAP data can be accessed through HSI tools FALCON and Integrated Case Management (ICM). ICE uses FALCON and ICM to collect data during raids and investigations. Moreover, ICM gives ICE agents access to intelligence platforms maintained by other federal and local law enforcement agencies, all of which help them develop targeting lists for raids. Everything from a person's school record, personal connections, biometric information, phone records, and family relationships end up in ICM.

Palantir Technologies, a company that is known for ICE contracts and management, designed FALCON and ICM for HSI and ERO.[38] FALCON also has a mobile component. All of these tools have been questioned for their potential to racially profile Black and Brown people.[39]

FOIA document showing Palantir developed FALCON (on file with author)

DHS continues to create concept papers for products and services that will tie in programs like BITMAP and EDDIE.[40]



Overall Concept and Goals

U.S. Immigration and Customs Enforcement

Additional BenefitsICE and DHS users will be able search and use these BITMAP submissions stored in EID from various IT products such as EAGLE, FALCON, and ICM. Currently the BITMAP submissions are only viewable using ID numbers searching IDENT and NCIC.This project will also update the biometric coding libraries for ICE. These commercial libraries have not been updated since the 2004 timeframe and do not support modern standards. This will allow for templateing IRIS images and facial recognition of Mug shots to support all submissions from EAGLE for these biometric modalities. Left and Right Profile collection would modernize the system to allow increased collection of subject booking photographs in EAGLE and the addition of SMT (Scar, Marks, and Tattoo) Photos.Modernizing the BITMAP process will allow increased collections on subjects that have criminal, gang associations, and immigration histories in other countries. If a alien travel to the United States it may shift the legal burden to the alien that they are not in violation of the INA when seeking admission, applying for an immigration benefit, or a visa to enter the United States. This could change the removal proceeding depending if a subject by prohibiting a subject from making a valid entry.Modernizing the BITMAP process will allow for the access to query tools of USCIS and CBP to be able to query more systems from EAGLE and EDDIE.

2015 BITMAP concept document that cites to EDDIE and EAGLE. 2018-ICLI-00008 2106

XII. CIVIL RIGHTS CONCERNS WITH EDDIE AND MOBILE BIOMETRICS

ICE has made invasive biometric collection a central part of everyday immigration enforcement, including raids and prosecutions. ICE uses EDDIE in raids where no one can see what is happening and no one can intervene. It is difficult to believe that abuses do not occur in those scenarios and that such technologies will have its largest impact on Black and Brown people who are suspected to be noncitizens.

In September 2020, DHS issued a proposed regulation re-defining and revamping biometrics so that biometric information - iris, DNA, fingerprints, palm prints, voiceprints, and other information - can be collected without accountability measures in place.[41] The regulation specifically referenced "EDDIE". This policy will have massive new implications for arrests and interrogations in public spaces. And, it impacts the ability to raise defensive claims in immigration court, including suppression cases.

- **EDDIE face and fingerprinting will promote racial profiling and abuse.** ICE agents use EDDIE to scan people first before making a decision to arrest. This sequence will foster racial profiling and abuse.

- **DHS can take fingerprints and face scans from noncitizens of any age (except lawful permanent residents).** On May 24, 2017, ICE released a policy eliminating age thresholds for "multimodal" biometric collection, meaning any biometrics that "will increase overall matching performance."[42] (In the past, DHS were permitted to take fingerprints from individuals between the ages of 14 and 79 years.) The administration will cement this practice through the September 2020 regulation.[43]

- **A 2014 HSI legal policy on mobile fingerprinting does little to explain when and how ICE may break the law when they utilize mobile fingerprinting. Moreover, the FOIA documents do not show whether ICE officers were following any policy at all.** In a policy document titled "HSI-Directive: Mandatory Booking of Arrestees using EAGLE," (April 23, 2014), HSI defines critical terms and creates procedures for the electronic booking of any person HSI arrests. The document specifies that if a person withdraws their consent to have their fingerprints taken, a warrant may be necessary.[44] In JFL's review of documents on EDDIE, ICE agents did not track whether ICE agents complied with protocols. (In the CNN video cited earlier and *Immigration Nation,* ICE agents did not appear to ask for consent.) In a complaint raised to the Office of Civil Rights and Civil Liberties (OCRCL) from Latino Union in Chicago, ICE stopped and detained people to take fingerprints and then decided who they wanted to arrest. This sequence of events lends itself to abuse and raises serious constitutional problems. More importantly, immigrants may be able to challenge detention or removal if ICE unlawfully captured fingerprints and face scans.

5.8. If, at any time during a consensual encounter, consent is withdrawn, a warrant may be necessary to take a subject's fingerprints. HSI SAs should take note of the following: In *Davis v. Mississippi*, 394 U.S. 721 (1969), the Supreme Court held that the taking of fingerprints is covered by the Fourth Amendment prohibition against unreasonable searches and seizures, and that fingerprints obtained as a result of an *illegal detention* are improperly admitted into evidence. In *Davis*, the defendant's detention was not based on a warrant or probable cause, and therefore constitutionally invalid. However, the court also indicated, "Detention for fingerprinting may constitute a much less serious intrusion upon personal security than other types of police searches and detentions. Fingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search." In his concurrence, Justice Harlan stated, "There may be circumstances... where compelled submission to fingerprinting would not amount to a violation of the Fourth Amendment, even in the absence of a warrant..." The necessity for a search warrant when obtaining fingerprints depends on the circumstances surrounding the lawfulness of the detention. The detention must be based on reasonable suspicion; otherwise it is likely constitutionally invalid.

- **USCIS, which is responsible for most immigration processing, wanted to use EDDIE on "defensive asylum applicants."**[45] In the excerpt below, ICE and USCIS officials discuss protocols for EDDIE use on asylum applicants. In this excerpt, DHS employees make damaging assumptions about an asylum applicant's credibility with ICE and USCIS.

Purpose: To identify how to approach the policy, privacy, and legal teams at both ICE and USCIS with the concept of ICE using EDDIE to collect biometric and biographic information about a subject on behalf of USCIS.

Background: LESA is currently holding discussions to define future functionality for ICE's mobile biometric and biographic collection tool, EDDIE. ICE has identified a potential use case, where ICE officers would use EDDIE to collect biometric and biographic information about encountered subjects who claim asylum or other benefits. ICE could potentially collect (but would not retain or store) the biographic information USCIS needs to address such cases and automatically send a message with the required information to USCIS.

Meeting Notes:

- ICE and USCIS have different standings as law enforcement entities (e.g., USCIS uses 10-prints for civil checks, whereas ICE conducts criminal checks)
  - ICE would conduct own procedures, but if the subject claims asylum, ICE will then collect the necessary information for USCIS and send it over
  - The **value-add** of this collaboration is that ICE avoids having to transport the subject to ASC to get printed
- Primary use: defensive asylum claimants
  - Affirmative asylum: there is only a two-week window between receiving the benefit and picking it up, during which USCIS would need 10-prints
- Use case: USCIS sends notice to ICE that they need the prints from a subject who is now in ICE custody
  - Notice has a two-number bar code
- ASCs are contractors and need a federal employee present when collecting biometrics, although they do not have to be Immigration Services
- If subject claims asylum, ICE will pull existing biographic information from EID, drop it into the necessary fields, and have the subject verify
  - Subjects might lie to ICE, but want to tell the truth to USCIS in order to get benefits

- **ICE has exploited the weakness of U.S. privacy laws to rapidly release new and evolving carceral technologies.** U.S. privacy laws do not help immigrants (except legal permanent residents) when their privacy rights are violated nor do they provide a meaningful way to access, review, or correct biometric information taken by ICE. ICE issues a decision on privacy risks of a new technology through a "Privacy Impact Assessment (PIA). PIAs, however, provide limited information to the public about a program and offer only an email to rectify a problem. ICE usually finds a way for invasive technologies to pass a privacy test; immigrants have no way to stop or access that information. As a result, personal and sensitive biometric information is now routinely shared with law enforcement agencies and private corporations that have contracts with ICE. For example, BITMAP took DNA from children without notifying parents and children. At first, they claimed DNA was needed to verify family relationships; now, DHS has expanded DNA collection to scenarios beyond family reunification.
- **We still know very little about the rules or regulations in how the agency deploys this technology.**

Many questions and concerns remain:

- Does ICE ask for consent before taking fingerprints or a facial scan?
- How do we know the subject has given consent?
- How do we know the encounter is "consensual"?
- What notice is provided to the respondent that these pictures and facial scans can be used against them?
- It appears that ICE captures facial scans and fingerprints, even when the agent elects not to arrest the person? What happens to that biometric data?
- What assurances do noncitizens and families have that this extremely personal information is not shared with other law enforcement?
- How do individuals review biometric data, and if necessary, remove or correct it?

XIII. CONCLUSIONS AND RECOMMENDATIONS

The use of mobile biometric devices in ICE immigration raids should raise serious national concern over civil rights violations, racial profiling, and privacy abuse. Over the last four years, the Trump administration built upon Obama-era programs and vastly expanded surveillance infrastructure, like EDDIE. ICE and CBP deployed military-grade weapons and technologies during the 2020 racial justice uprisings on civilian protesters, including Black and Brown communities.[46]

Biometric collection devices are not "less violent." They supercharge raids and surveillance and should be seen as an extension of mass incarceration and surveillance of Black and Brown communities. We must raise the alarm on the exploding market for prison and policing technologies being bought by ICE and police. Several corporations, such as NEC and Dataworks Plus, have created the next iteration of fingerprinting and face scanners for DHS and DOD that are easier to use than NeoScan45. Data sweeps, sharing, and scraping amongst corporations, police, and ICE will be used to make vast new target lists for raids, deportations, jail, and tracking.

Palantir, Clearview, Northrup Grumann, NEC, and many others are making millions from DHS contracts. The incoming administration can reverse course to stop the windfall of billions of dollars to corporations that advance intrusive, exploitative tech surveillance. In many cases, employees from these corporations are making decisions about the data themselves - decisions that could change a removal hearing, a raid at a day laborer corner, or a DACA application.

In September 2020, DHS released a sweeping regulation that sets no verifiable limits on how DHS collects, handles, stores, and shares biometric data with federal and state entities, foreign governments, and private corporations. EDDIE was specifically named as a core mobile biometric function. The FY2021 proposed budgets are loaded with surveillance, but how ICE uses its multi-billion dollar budget is shrouded in secrecy.[47] Most recently, the incoming administration identified information sharing and collection as a key tool to control the border and immigration.[48]

Everyone has a right to understand and monitor how their bodies and other personal data are collected and used. We already know that Black, Brown, and immigrant communities are subject to higher levels of law enforcement scrutiny.

We make the following recommendations:

1. **DHS must halt the use of mobile biometrics collection and data sharing.** ICE uses EDDIE mobile fingerprinting to accelerate raids and deportations, but they disclose very little about their data sharing partners, such as other federal agencies, local law enforcement, and private companies. ICE makes decisions to arrest and detain after pictures and fingerprints are captured, raising serious questions about abuse and racial profiling. DHS lacks structural accountability mechanisms to oversee and manage these technologies effectively. Even their own statistical sheets did not measure adherence to any oversight mechanisms.

2. **Congress must halt funding for EDDIE and BITMAP.** Biometric collection technologies operate without limit, and Congress must investigate and disclose technologies that have such a massive impact on the public. These programs have operated with bipartisan support and without accountability and oversight for 7 years, costing the public millions of dollars.

Congress should not fund these programs or similar programs until more is known about the programs and the companies that make its products.

3. **Congress should halt funding of OBIM, an agency that has flown under accountability radars for too long.** OBIM is responsible for managing EDDIE acquired data, but it is extremely difficult to find out more about their role and the agents or contractors managing the data. They are also responsible for deploying HART, the new DHS biometric database that will contain millions of faces, iris scans, fingerprints, biographic, family, and community relationships. The public must know more about the functions, responsibilities, and data sharing protocols being created by OBIM for EDDIE, BITMAP, and HART.

4. **DHS should roll back regulations and privacy exclusions for biographic and biometric programs.** DHS and ICE overused privacy exemptions to immunize themselves from privacy laws related to the creation and deployment of biometric programs. The administration should rescind these exclusions in favor of transparency to the public.

XIV. ENDNOTES

1. FOIA Documents: DHS-001-HQFO-00676-000148 to DHS-001-HQFO-00676-000160

2. This report presents the best-known information regarding EDDIE and mobile biometrics in ICE from 2014 through mid-2018. It is based in large part on the US federal government's response to a Freedom of Information Act lawsuit brought by the National Immigration Project of the National Lawyers Guild and Mijente on information regarding ICE's use of mobile biometrics. The FOIA request focused on the following issues: (1) Proliferation of mobile biometric devices and applications in ICE enforcement actions, (2) Information on use of mobile biometric devices and applications in immigration actions, (3) Mechanisms for accountability and oversight of use of mobile biometric devices, (4) Concerns over civil rights, racial profiling, and privacy rights given its increased use.

3. EDDIE raids can be seen in Episodes 1 and 3 of Netflix's *Immigration Nation* which showed ICE agents using EDDIE to take fingerprints and photos of immigrants during home raids and on the street.

4. Notice of proposed rulemaking, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (Sept. 11, 2020), https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf. "Currently, when ICE arrests an alien, fingerprints are collected as part of the process of building an A-file on the alien. A handheld mobile biometrics application called "EDDIE" is used to facilitate the collection and recordkeeping of aliens in ICE custody. This handheld application effectively and efficiently collects fingerprints and photographs in about 30 seconds, which are then transferred to IDENT."

5. ICE FOIA 2018-ICLI-00008, p. 2362.

6. ICE FOIA 2018-ICLI-00008, P 2303

7. Privacy Impact Assessment Update for the Enforcement Integrated Database (EID) – EAGLE, EDDIE, and DAVID DHS/ICE/PIA-015(j), May 14, 2019; https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-eid-may2019.pdf. Specifically, EDDIE assists ICE agents and officers to lawfully collect an investigation subject's fingerprints and photograph using a mobile device, and immediately query other government databases to determine if they contain the same fingerprints as those collected by ICE. Aside from the subject's fingerprints and photograph, EDDIE also collects the PICS ID4 of the agent or officer who created the entry, transaction information (dates and times when ICE queries other government databases and when the results are returned), and EDDIE can verify the identity of a subject presumably already known to ICE and is also used to identify a subject who is unknown to ICE by querying other government databases.

8. Id.

9. ICE FOIA Docs, 2018-ICLI-00008, P172

10. ICE FOIA 2018-ICLI-00008, P3

11. ICE FOIA, 2018-ICLI-00008, P172

12. Privacy Impact Assessment for the Law Enforcement Information Sharing Service (LEIS Service), DHS/ICE/PIA-051June 28, 2019, p. 2 (last visited https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-leiss-july2019_0.pdf)

13. The ICE Integrated Product Team (IPT) for mobile applications participated in EDDIE development. The ICE IPT includes the OCIO Architecture (Technical, Section 508 Compliance), OCIO Info Assurance Division (IAD), ICE Privacy Office (IPO), ICE Office of Public Affairs (OPA), ICE Office of the Principal Legal Advisor (OPLA), ICE Office of Professional Responsibility (OPR), ICE Governance - Office of the Component Acquisition Executive (OCAE), and Portfolio Support Office (PSO) Lead. A key approval entity is ICE IT/Infrastructure Executive Steering Committee (ESC) which gave approval for EDDIE to begin development and rollout. Rollout approval leads to an acquisition.

14. EDDIE operates technically through the "Good container" for distribution and requires four accounts to activate: PICS ID (allows you to log into ENFORCE), Good for Enterprise (also allows email client on iPhone,iPad), Good Dynamics (a back end license), Good AppCentral (ICE App Store). A user needs usernames and passwords to all four to download EDDIE.

15. ICE FOIA Docs: 2018-ICLI-00008, P. 2311. Documents suggested tracking mechanisms to count the exact number of devices were low.

16. Kanowitz, Stephanie, "ICE agents collect biometric ID in the field," GCN, Sept 21, 2016, (last visited on October 2020 https://gcn.com/articles/2016/09/21/dig-it-ice-eddie.aspx).

17. ICE FOIA 2018-ICLI-00008, P77

18. ICE FOIA doc, 2018-ICLI-00008, P2362

19. NEC website on mobile fingerprinting. https://www.necam.com/AdvancedRecognitionSystems/Products/NeoScan45/

20. https://www.usaspending.gov/award/CONT_AWD_HSCETE14J00287_7012_HSHQDC13D00023_7001

21. GAI and NEC Press Release on EDDIE. https://gov-acq.com/press-release/gai-and-nec-help-u-s-immigration-and-customs-enforcement-with-mobile-biometric-technology-to-assist-in-border-enforcement-efforts/

22. U.S. contract awards. https://www.usaspending.gov/award/CONT_AWD_HSCETC12F00005_7012_HSCETC11A00006_7012

23. Wexler Technical Solutions has gone beyond its contract with ICE and is marketing EDDIE as a product called WTS IDENTIFY and offering it up under a GSA contract vehicle. Screenshots from WTS's website are included below. WTS IDENTIFY is a mirror image of the EDDIE.

24. ICE FOIA doc, 2018-ICLI-00008, P2311.

25. ICE FOIA doc, 2018-ICLI-00008, P2399-2400; ICE FOIA doc, 2018-ICLI-00008, P709-710; ICE FOIA doc, 2018-ICLI-00008, P1725-1729.

26. ICE FOIA doc, 2018-ICLI-00008, P2295

27. ICE FOIA doc, 2018-ICLI-00008, P2311. For references to Alternatives to Detention agents, see ICE FOIA 2018-ICLI-0008, P2128-2137.

28. Office of Biometric Identity Management, Department of Homeland Security, https://www.dhs.gov/obim (last published date August 27, 2020)

29. ICE FOIA doc, 2018-ICLI-00008, 2095

30. https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis-ngi-risc. See also 2018-ICLI-00008, P2484.

31. This information was shared in an HQ email for an "Eddy" screening after a shooting in Prince George's County, Maryland. ICE FOIA2018-ICLI-00008, P2474

32. "International Week: An Inside Look at International Operations," HSI. https://www.ice.gov/features/international-week. BITMAP works with another program called JAIME. JAIME will be a tool to allow foreign vetted Law Enforcement personnel the ability to submit type 14 biometric capture in remote environments outside of the DHS network. It will be an independent biometric application for collection and enrollment under the BITMAP program. This means law enforcement officers in other countries will feed biometric information into DHS databases.

33. ICE FOIA 2018-ICLI-00008, P671-679.

34. This number was disclosed by HSI officials in a 2020 business and contractor conference about the use of biometrics in law enforcement.

35. Washington, John and Jacqueline Stevens, "*Democratic Representative pushed to create a massive migrant health database no one wants*, The Intercept, Jan. 4, 2020. Last visited October 10, 2020. https://theintercept.com/2020/01/04/border-patrol-cbp-migrant-health-database/

36. Jabed v. Keeton, 2019 WL 6320385 (Nov. 26, 2019); Imon v. Keeton, 2020 WL 4284378 (July 27, 2020)

37. See H.R. 3377 (2019-2020), H.R. 6439 (2018-2019). https://www.congress.gov/115/crpt/hrpt909/CRPT-115hrpt909.pdf

38. Woodman, Spencer. "Palantir provides the engine for Donald Trump's Deportation Machine," The Intercept, March 2, 2017 (last visited October 2020 at https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/).

39. Bajak, Frank, "Secretive, never profitable Palantir makes market debut," SF Gate, September 30, 2020, (last visited https://www.sfgate.com/news/article/Secretive-never-profitable-Palantir-makes-its-15608150.php.)

40. ICE FOIA 2018-ICLI-00008 2106.

41. "Collection and Use of Biometrics by USCIS," 85 FR 56338, (September 13, 2020). https://www.federalregister.gov/documents/2020/09/11/2020-19145/collection-and-use-of-biometrics-by-us-citizenship-and-immigration-services

42. "DHS Biometrics Expansion for Improved Identification and Encounter Management," DHS, May 24, 2017 (available at https://www.dhs.gov/sites/default/files/publications/dhs_biometrics_expansion.pdf).

43. As of September 2020, ICE will institute a regulation memorializing this policy.

---

44. ICE FOIA 2018-ICLI-00008, P739.

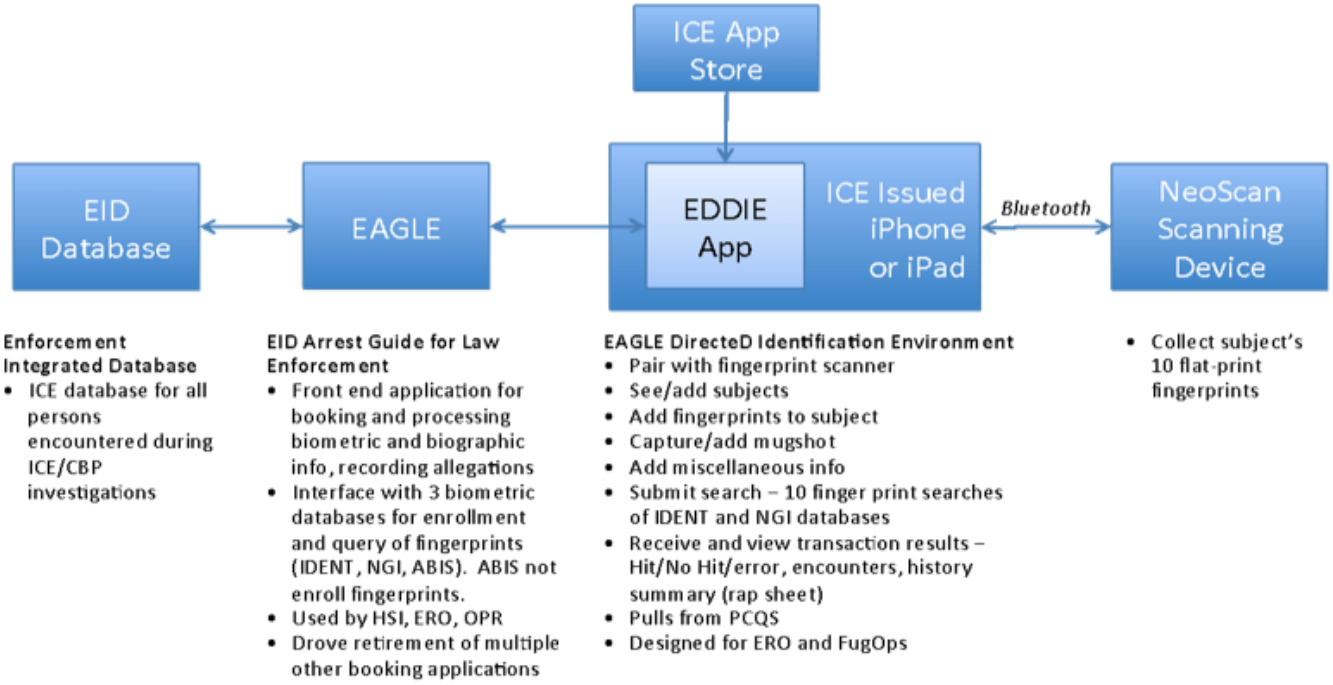
45. ICE FOIA 2018-ICLI-00008, 2476-2477

46. Holt, Kris. "CBP Flew a Predator Drone Over Minneapolis Amid George Floyd Protests," Forbes, May 29, 2020. https://www.forbes.com/sites/krisholt/2020/05/29/cbp-predator-drone-minneapolis-george-floyd-aclu/?sh=2b6bdc2740fa. Winter, Jana. "Leaked document reveals details of federal law enforcement patrolling Washington amid protests,"Yahoo News, June 5, 2020, https://news.yahoo.com/exclusive-leaked-document-reveals-details-of-federal-law-enforcement-patrolling-washington-amid-protests-154138680.html; Aleaziz, Hamed, Adolfo Flores and Kendall Taggart, "Former Officials Say The Elite Border Patrol Unit Sent To Confront Portland Protesters Is Like A "Fish Out Of Water", BuzzFeedNews, July 24, 2020. https://www.buzzfeednews.com/article/hamedaleaziz/elite-ice-unit-versus-portland-protesters-controversy.

47. Elis, Niv. "Senate releases spending bills, setting up negotiations for December deal," The Hill (Nov. 11, 2020), last visited https://thehill.com/policy/finance/525277-senate-releases-spending-bills-setting-up-negotiations-for-december-deal. "Explanatory Statement for the Homeland Security Appropriations Bill, 2021," https://www.appropriations.senate.gov/imo/media/doc/HSRept.pdf; H.R.8337 - Continuing Appropriations Act, 2021 and Other Extensions Act, https://www.congress.gov/bill/116th-congress/house-bill/8337.

48. https://joebiden.com/immigration/

XV. APPENDIX A: EDDIE USE INFORMATION FLOW



Utilization of EDDIE in the field includes the following steps:

1. Pair NeoScan with iPhone/iPad that has EDDIE application over Bluetooth

User must pair the NeoScan device first. If prints are collected before pairing, the prints will be erased when it is paired with an iPhone/iPad.

2. Log in to EDDIE

3. View the Subject List screen in EDDIE app

EDDIE Subject List screen is the main screen in application. Either see list of subjects user created or subjects assigned to user's AOR. Each subject listed on Subject screen represents a transaction where biometric data was captured for a specific individual at a specific point and time. User can toggle between the two views of Subject List screen by tapping 'Your Subjects' or 'Site Subjects'.

Subject Details Screen - displays all information entered for a subject as well as high-level results of transaction submitted from EDDIE. EDDIE has three detail categories: images (fingerprints and mugshots), transactions, miscellaneous information.

4. Add new subject

5. Capture and add fingerprints to subject

EDDIE will display "Waiting for fingerprints from device..." which prompts user to use NeoScan. After fingerprints are successfully captured, EDDIE will display "Transferring fingerprints". Fingerprints are captured and transferred to EDDIE one by one. NeoScan blinks red LED when ready to collect the next required print.

When all required prints are captured, NeoScan blinks green lights and user transferred back to Subject Details screen in EDDIE.

6. Add mugshot

Picture taken from iPhone or iPad, not NeoScan device. Collecting mugshot from subject is required so EDDIE user can differentiate between subjects in the Subject List screen

7. Add miscellaneous information

User can enter Description (name, A#), capture location via iPhone/iPad location services, auto-populate user's ENCORCE ID. Users are requested to type subject's full name and complete A# in a standard format, e.g., JoseOchoa123456789

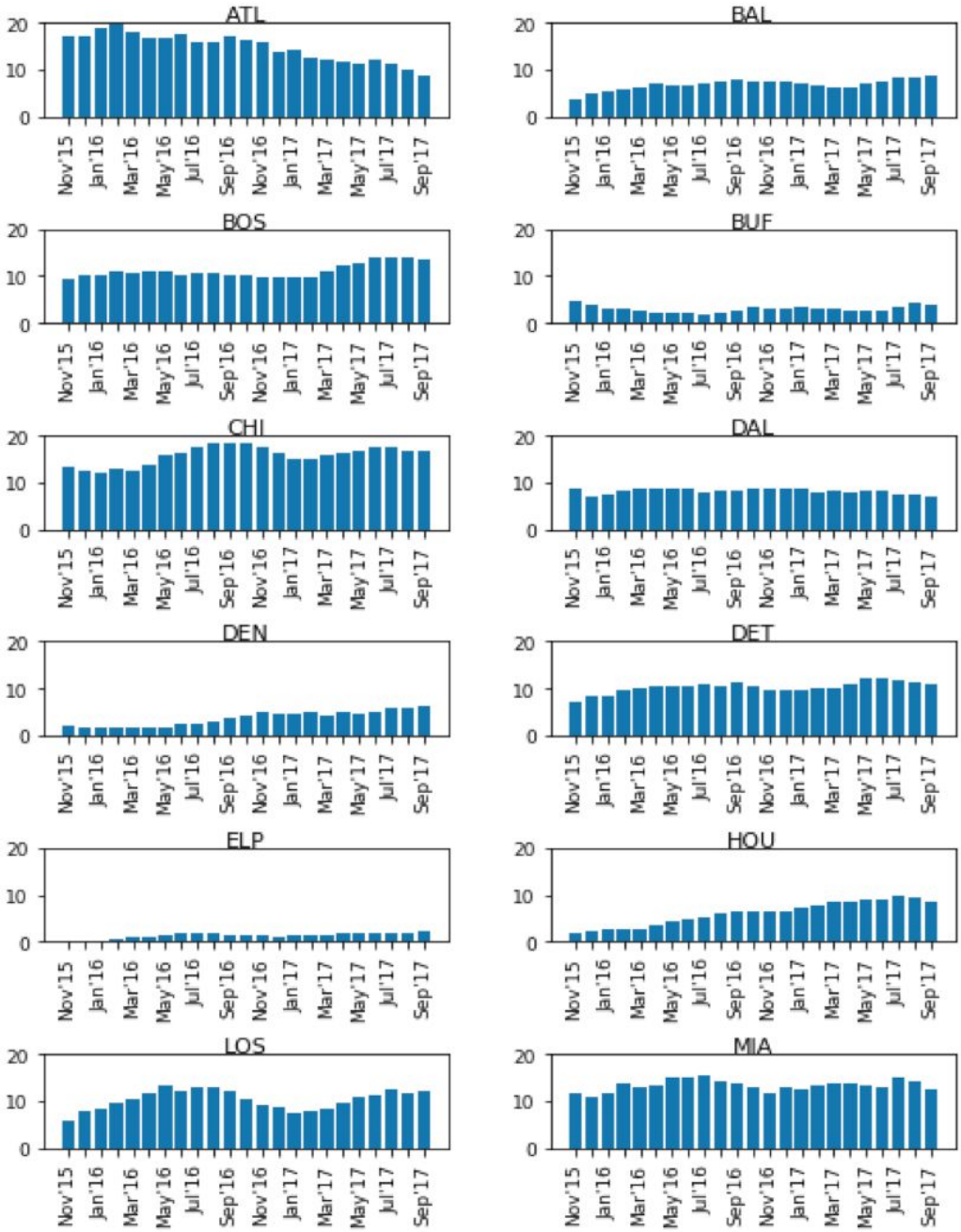
8. Submit biometric search transaction

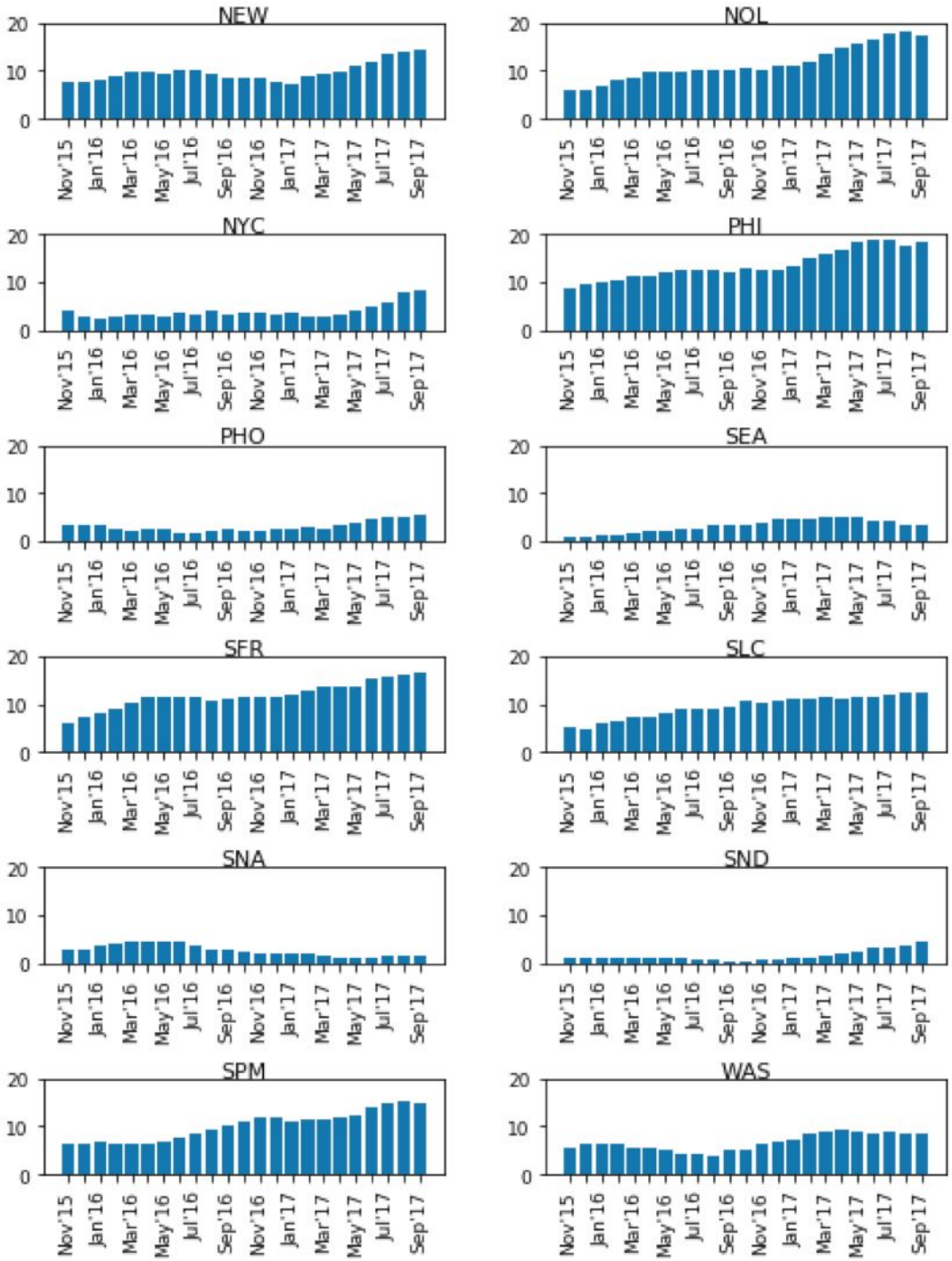
To perform biometric search, need to create a new subject and assign biometrics (fingerprint and mug shot) in the app, add fingerprints from NeoScan and then submit subject info to IDENT. The response is shown in the Subject List screen under “Transactions”.

9. Receive and view transaction results back

Response & Encounters Screen - if fingerprints result in a hit in IDENT (this is for v1.0, later does this also include NGI), Response screen will display biographical data including names, FBI number, and FIN number among other data points. There are various types of hits: responses are ‘No Hit’ (NH) or various levels of ‘Hit’ (H1, H2, H3): If subject has been encountered before, list of previous IDENT encounters will also be displayed. Specific details of any encounter may be viewed by tapping on it. A booking record is NOT created at the time of subject creation in EDDIE.

XV. APPENDIX B: USE OF EDDIE BY AORS ("FIELD OFFICES") FROM 11/15 THROUGH 9/17




NEW
NOL
NYC
PHI
PHO
SEA
SFR
SLC
SNA
SND
SPM
WAS
0
10
20
Nov'15
Jan'16
Mar'16
May'16
Jul'16
Sep'16
Nov'16
Jan'17
Mar'17
May'17
Jul'17
Sep'17