

February 2018

TABLE OF CONTENTS

Introduction 1
Enforcement Updates 1
Some Cases Challenging DHS’ Use of Technology against Immigrants 3
Gang Databases..... 3
Important Cases at the Supreme Court 4
Corporate, DHS and DOJ Technology Conferences and Meetings 5

INTRODUCTION

Surveillance and technology-driven surveillance is the emerging centerpiece of DHS enforcement and becoming big business for private companies. From raids to visa vetting, the Department of Homeland Security has invested in scanning technology, such as fingerprint, facial, and iris technology, to carry out such enforcement tactics.

ICE uses these technologies to identify and target immigrants and their families for deportation or prosecution . DHS is deploying surveillance technology in both the interior and the border – for people who are undocumented and who have green cards and US citizens.

Meanwhile, DHS and the DOJ are putting weak, if any, limitations on how these technologies are used against immigrants and their communities, which are disproportionately communities of color.

This newsletter provides critical information about technology used in DHS interior enforcement and will include:

- use of these technologies companies that sell these products and services to DHS
- advocacy efforts to limit the expansion of these technologies and create accountability
- meetings and events on biometric and surveillance technologies legal developments

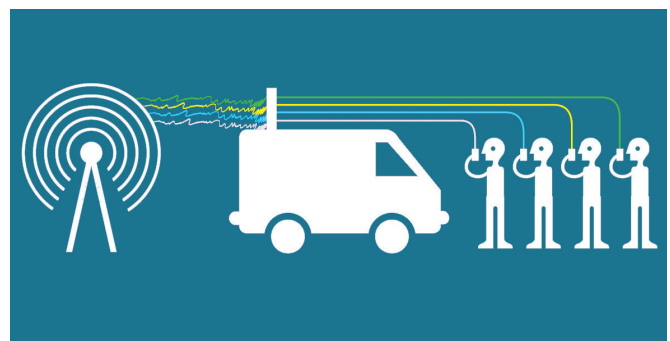
ENFORCEMENT UPDATES

Stingray Use in Detroit to Arrest Immigrant

(May 18, 2017)

DHS used a Stingray to arrest an undocumented person. A stingray is a surveillance tool used by federal agents to trick a cell phone into providing location data. At the same time it can interrupt cell service of all devices around the phone. Usually, you need a warrant to use a Stingray. In this case, they arrested someone with a previous deportation order for the federal charge of illegal reentry.

<http://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/>



StingRay cell site simulators can be used to perform a man-in-the-middle attack on mobile phones. Illustration courtesy of <https://www.eff.org/deeplinks/2016/08/fcc-created-stingray-problem-now-it-needs-fix-it>

DHS Use of Private Datamining Contractors to Identify Targets for Raids and their Location

DHS uses commercial vendors to obtain targets for raids and other operations. These commercial vendors look for information on criminal history and vehicle registration sites. For example, an investigations unit within ICE called the National Criminal Analysis and Targeting Center (NCATC). On a weekly basis, ICE provides names and dates of birth to the commercial data vendor in an electronic format and then the vendor searches for identifying information like biographical information, criminal history, criminal case history, and vehicle information (including vehicle registration information). During Operation Safe Cities, ICE referenced using NCATC.

<https://www.dhs.gov/publication/dhsicepia-048-data-analysis-system-das>



DHS and Social Media Collection

(9/26/2017)

DHS is collecting social media information on all immigrants, including legal permanent residents and naturalized citizens. This means public handles, Facebook, and Twitter information may be collected and used against noncitizens applying for immigration relief.

<http://thehill.com/policy/national-security/352421-dhs-planning-to-collect-social-media-info-on-all-immigrants>

Millions of dollars will be spent on companies who do social media “mining.” Already, one company in Virginia was awarded a contract by DHS.

<https://www.forbes.com/sites/thomasbrewster/2017/09/27/trump-immigration-social-media-surveillance-giant-oak-penlink-palantir/#41e22b-7f3e3b>

To learn more about how to better protect yourself, please refer to our social media advisory at:

https://www.nationalimmigrationproject.org/PDFs/community/2017_03Apr_comm-adv-social.pdf

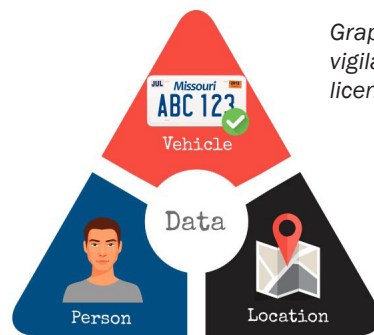
DHS is Collecting License Plate Information from a Commercial Vendor, Vigilant Solutions

(January 2018)

ICE announced that it will have access to license plate information collected by a business named Vigilant Solutions. Vigilant collects license plate information from vehicle repo companies, toll road cameras, parking lot cameras and law enforcement agencies and through their own License Plate Readers (LPRs). Twenty-five states and 24 of the top 30 most populous metropolitan statistical areas feed into Vigilant’s database.

The list of states is not public but the Electronic Frontier Foundation has found a group of counties using it in California.

<https://www.eff.org/deeplinks/2018/01/ice-accesses-massive-amount-license-plate-data-will-california-take-action>



Graphic from <https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/>

Advocacy Update

The City of Alameda rejected a Vigilant contract after learning of the significant privacy concerns posed by the technology within the city.

<https://oaklandprivacy.org/2018/02/07/city-of-alameda-rejects-alpr-contract-with-vigilant/>

SOME CASES CHALLENGING DHS' USE OF TECHNOLOGY AGAINST IMMIGRANTS

Mobile Fingerprinting Biometric Technology Freedom of Information Act (FOIA) Lawsuit

(12/5/2017)

Mijente and the National Immigration Project of the NLG filed a Freedom of Information Act request about mobile biometric technology after hearing of its use in several raids, and a FOIA lawsuit followed. Usually, immigrants are “booked” at a local jail to get fingerprints; now immigrants are being “booked” where they are arrested. This will make deportation happen a lot faster.

https://www.nationalimmigrationproject.org/pr/2017_05Dec_nipnlg-v-icedhs-biometric.html

Companies like NEC are selling biometric technology services and products to DHS.

<https://integratedbiometrics.com/cnn-story-on-ice-agents-features-neoscan-45-from-nec/>

GANG DATABASES

Chicago

Organized Communities Against Deportation (OCAD) and Black Youth Project 100 are working to end gang databases in Chicago that have fostered racial profiling for years. OCAD leads advocacy efforts to close loopholes in sanctuary city policies in Chicago for black and brown immigrants suspected of being in gangs. They are leading advocacy efforts and spearheading legal and advocacy work around gang databases in Chicago. One example is the case of Wilmer Catalan-Ramirez, a family man and mechanic, who was arrested and detained by ICE after being falsely included in the Chicago gang Database. A victim of a drive-by shooting, he suffered numerous injuries while detained. After months of sustained organizing by OCAD and legal work, ICE released Wilmer. Attorneys working on his civil lawsuit settled the case in January 2018.

Learn more about Wilmer at www.organizedcommunities.org.

His family and organizers at OCAD have set up a fund for Wilmer’s recovery:

<https://www.youcaring.com/wilmercatalan-ramirezandhisfamily-1075617>

Catalan-Ramirez v. ICE, City of Chicago

Case: 1:17-cv-03258 - SETTLED

The MacArthur Justice Center and The National Immigration Project of the NLG and the filed suit against ICE and the City of Chicago for Wilmer Catalan-Ramirez, whose false inclusion in the Chicago Police Department’s “Gang Database” and the sharing of that information with U.S. Immigration and Customs Enforcement (ICE) triggered a nightmarish chain of events that left him imprisoned, in severe physical pain and mental anguish, and fighting deportation.

https://www.nationalimmigrationproject.org/pr/2017_01May_wilmer-v-chicago.html



Wilmer Catalan-Ramirez with his family after being released. Photo courtesy of Organized Communities against Deportation (OCAD)

Pedrote-Salinas v. Superintendent Billie Johnson, et. al

Case: 1:17-cv-05093

This case involves a young man stripped of DACA because of his inclusion in the Chicago gang database. Mr. Pedrote-Salinas sued to learn more about how Chicago collected that information.

http://www.macarthurjusticecenter.org/uploads/rsmjc/documents/luis_lawsuit.pdf

Nationwide

Tattoo Recognition Technology Program FOIA Lawsuit

(11/30/2017)



The Electronic Frontier Foundation filed a FOIA lawsuit in Washington, DC against DHS, FBI and DOJ to learn more about the “Tattoo Recognition Technology Program.” This program’s goal is to scan tattoos on someone’s body and to classify them into particular groups, like gangs. This scanning technology will have an impact on immigrants because they will be used to predict whether someone is associated with a group or has gang affiliations and can be used to deny green cards or other immigration benefits.

<https://www.eff.org/press/releases/eff-demands-information-about-secretive-government-tattoo-recognition-technology>



IMPORTANT CASES AT THE SUPREME COURT

Carpenter vs. United States at the Supreme Court

(Argued on 11/29/2017)

This case involves the following issue: Whether the government, without a warrant, can effectively trace a person’s movements in public for months on end by demanding 127 days of the geolocational data—known as cell-site location information—that mobile phones beam out 24 hours a day. This is arguably one of the biggest privacy decisions of this decade. If the government is not required to get a warrant, then it will be much easier for the government to surveil and track people without a good reason.

The court will make a decision about this case in spring 2018. You can read about the case here:

<https://www.theatlantic.com/politics/archive/2017/11/bipartisanship-supreme-court/547124/>

<http://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/>

CORPORATE, DHS AND DOJ TECHNOLOGY CONFERENCES AND MEETING

DHS Rallies

In these rallies, DHS meets with industry and technology companies to explore and experiment with new DHS technologies. Several “rallies” are planned each year to explore and implement new biometric tools for “law enforcement insertion.”

The first rally will be held in Upper Marlboro, Maryland in March 2018 at a testing site called the Maryland Testing Facility and will evaluate face and iris biometric systems.

<https://www.dhs.gov/science-and-technology/news/2017/11/08/news-release-dhs-st-announces-biometric-technology-rallies>

<http://mdtf.org/rally/rally/DetailSchedule.html>

FBI Compact Council



This council is a group of state and local law enforcement agencies who discuss how and what information is shared with the FBI NCIC database (fingerprint, iris pictures, etc). ICE, USCIS, CBP are some of the

users of this system along with all the police and jail agencies in the United States. This Council designs and implement policy, usually without any community input. Deportation orders are entered into the NCIC database. It is expected that they will debate whether ICE and USCIS can have access to biometric information collected for noncriminal employment purposes – for example, teachers and nannies provide fingerprints for background data purposes to see if they have any criminal history that would bar them from the job.

Timing

The FBI Compact Council members meet several times a year. Their meetings start in March 2018.

<https://www.fbi.gov/services/cjis/compact-council/upcoming-meetings>

Relevant reading material:

<https://www.thedailybeast.com/will-ice-get-its-hands-on-the-fbis-fingerprints>

Corporate Conferences

NEC: AFIS Internet Users Conference:
August 26-29, 2018 in Reston, VA

This is a massive conference organized by NEC Corporation to explore biometric “solutions” from “identification professionals.”

<https://www.necam.com/AdvancedRecognition-Systems/AFIS2018/>

Biometrics for Government and Law Enforcement Conference

February 26-28, 2018 in Washington, DC,

This conference has leaders from DHS and other federal agencies to talk about their biometric needs.

