WHO'S BEHIND ICE?

THE TECH AND DATA COMPANIES FUELING DEPORTATIONS

national IMMIGRATION project of the National Lawyers Guild

IDP IMMIGRANT DEFENSE PROJECT

mijente

Who's Behind ICE?

The Tech Companies Fueling Deportations

Tech is transforming immigration enforcement. As advocates have known for some time, the immigration and criminal justice systems have powerful allies in Silicon Valley and Congress, with ***technology companies playing an increasingly central role in facilitating the expansion and acceleration of arrests, detentions, and deportations.*** *What is less known outside of Silicon Valley is the long history of the technology industry's "revolving door" relationship with federal agencies, how the technology industry and its products and services are now actually circumventing city- and state-level protections for vulnerable communities, and what we can do to expose and hold these actors accountable.*

Mijente, the National Immigration Project, and the Immigrant Defense Project — immigration and Latinx-focused organizations working at the intersection of new technology, policing, and immigration — commissioned Empower LLC to undertake critical research about the multi-layered technology infrastructure behind the accelerated and expansive immigration enforcement we're seeing today, and the companies that are behind it. The report opens a window into the Department of Homeland Security's (DHS) plans for immigration policing through a scheme of tech and database policing, the mass scale and scope of the tech-based systems, the contracts that support it, and the connections between Washington, D.C., and Silicon Valley. It surveys and investigates the key contracts that technology companies have with DHS, particularly within Immigration and Customs Enforcement (ICE), and their success in signing new contracts through intensive and expensive lobbying.

Targeting Immigrants is Big Business

Immigrant communities and overpoliced communities now face unprecedented levels of surveillance, detention and deportation under President Trump, Attorney General Jeff Sessions, DHS, and its sub-agency ICE. Tech innovation and infrastructure makes this possible, allowing immigration enforcement to rely on policing through huge databases, computer programs, tech employees analyzing big data, and shareable cloud-based storage. These systems accumulate unprecedented amounts of personal and private information and enable the rapid expansion of information-sharing capabilities among city, state, and regional law enforcement agencies, as well as some foreign governments, for the purpose of finding, deporting, and detaining immigrants.

Immigration enforcement and detention is now big business for Silicon Valley. ICE, DHS, and many other law enforcement agencies spend billions of taxpayer dollars on procuring and maintaining these new systems. Currently, about 10 percent of the DHS $44 billion budget is dedicated to data management. **A handful of huge corporations, like Amazon Web Services and Palantir, have built a "revolving door" to develop and entrench Silicon Valley's role in fueling the incarceration and deportation regime.** Unchecked, these tech companies will continue to do the government's bidding in developing the systems that target and punish *en masse* those it deems "undesirable" — immigrants, people of color, the incarcerated and formerly incarcerated, activists, and others. It is

deeply troubling that at the same time these corporations characterize these services and products as business ventures that are free from bias, racism, profiling, and abuse, while being highly profitable.

Trump and Sessions are clear about their agenda. They are going after immigrants, naturalized and undocumented alike, as part of a larger white supremacist project. Yet, as resistance to this administration continues to grow, we must all ask ourselves where we stand and ask others what side they are on. **Dismantling the lucrative relationship between tech and ICE must be a key component of the movement to push back against the Trump-Sessions agenda, to #AbolishICE, and to defend our families and communities.**

No Such Thing as Sanctuary

ICE cannot develop or operate its massive information systems without the technology industry and its products and services. And as the Trump administration increases the mandate and secures more resources for the agency, ICE has been soliciting companies to staff up, service, and resource its needs to manage the huge amounts of information it collects or buys on immigrants and the people connected with them. The massive government cash infusion has even birthed new companies focused specifically on getting ICE contracts and expanded monopoly powers of major corporations in Silicon Valley, such as Palantir and Amazon. And elected officials are expanding that footprint by proposing legislation that will facilitate ICE contracting and expand biometric collection.

ICE is preparing to use tech for mass deportation at an unprecedented scale that could make "Sanctuary" city- and state-level protections obsolete. As the report reveals, ICE wants to organize mass personal information it buys from private vendors, such as license plate information; collect intimate biometric information in mass quantities, such as fingerprints, iris scans, facial recognition software; buy the "cloud" space to store the data and hire people to analyze the mass data information - all for surveilling, arresting and deporting immigrants. These programs have enormous implications for protective policies in cities and states by making the separation of information impossible, granting full access to Trump's federal police force.

The report highlights **Amazon and Palantir as two companies that are at the forefront of these developments, providing the collection, storage, and management of the vast amount of information required by ICE to increase its reach to the levels promised by the Trump administration. Both companies have enabled DHS to apply new**

technologies and expand its data-sharing capabilities to undermine and get around any local protections that were hard-fought and won by immigrant rights organizers. This interoperability has effectively expanded the reach of immigration enforcement by rendering detentions and deportations more likely to occur. Through intense lobbying of policymakers and law enforcement officials, Amazon and Palantir have secured a role as the backbone for the federal government's immigration and law enforcement dragnet, allowing them to pursue multi-billion dollar government contracts in various agencies at every level of law enforcement and defense.

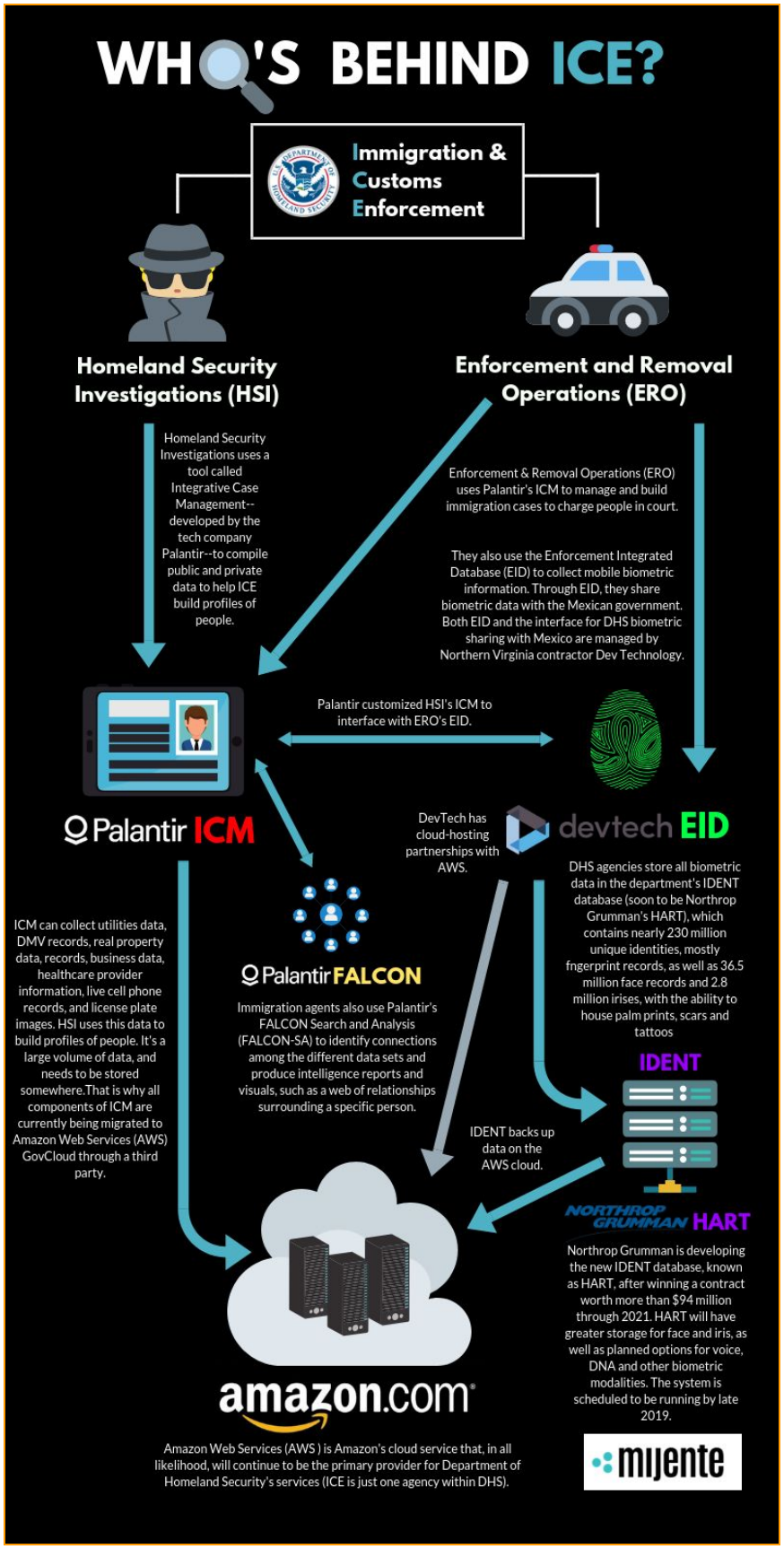
Data Drives Deportation Raids

Palantir is building ICE's case management software — tech that allows immigration agents to scour regional, local, state, and federal databases across the country, build profiles of immigrants and their friends and family based on both private and public information, and use those profiles to surveil, track, and ultimately deport immigrants. Their technical services have led to:

- Dangerous acceleration of surveillance technology at the hands of police and prosecutors to target and build profiles of people — an infrastructure that also fuels discriminatory policing practices targeting people of color;
- Increased mining and accumulation of data from a myriad of sources, including utility bills, DMV records, business and property data, healthcare provider information, live cell phone records, biometric databases, and social media accounts; and
- Unprecedented data sharing between every level of law enforcement that undermines Sanctuary City policies.

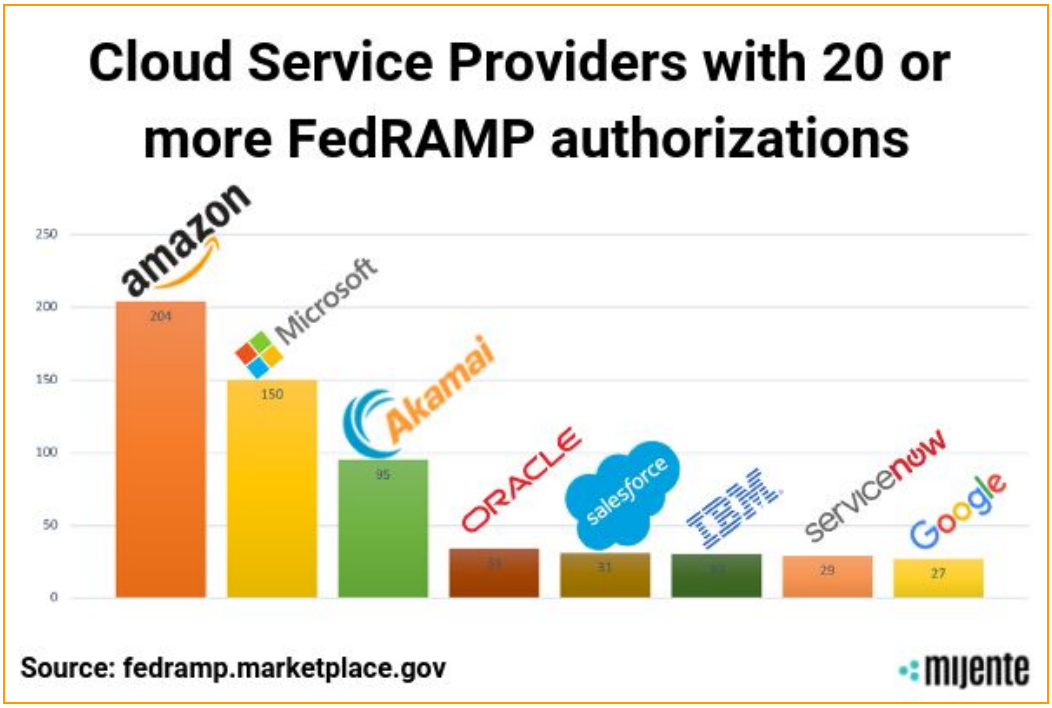
Sanctuary cities have and will struggle to fully protect their immigrant communities, because local law enforcement departments use the same Palantir-created data systems as ICE. That means that every time local law enforcement uses their systems, they are, in effect, feeding information that ICE can use to conduct raids. Both Palantir's Integrated Case Management (ICM) and FALCON Search and Analysis (FALCON-SA) systems ensure these capabilities, allowing for more pinpointed enforcement actions. Local police can easily access federal data on particular individuals and help build national profiles of individuals that are then used by ICE. Federal immigration agents can even access local police information, like license plate data, through shared systems even when local jurisdictions have chosen not to cooperate with federal immigration enforcement.

At the same time, hundreds of small to mid-sized corporations are competing to build information-sharing platform and software programs for ICE that operate like these models. Dev Technology, a Maryland-based company earning millions from ICE and Customs and Border Patrol, is building biometric tracking programs for ICE for use in Mexico - ostensibly for use against all migrants traveling in Mexico. Forensic Logic, the maker of COPLINK, a program used by over 5,100 law enforcement agencies across the country and hosted on Amazon Web Services (AWS), was designed to be compatible with federal immigration databases. COPLINK contains diverse information on individuals, organizations, and vehicles, and will allow ICE unprecedented access to information about employers, "associates," and hangout spots.


WHO'S BEHIND ICE?
Immigration & Customs Enforcement
Homeland Security Investigations (HSI)
Enforcement and Removal Operations (ERO)
Homeland Security Investigations uses a tool called Integrative Case Management--developed by the tech company Palantir--to compile public and private data to help ICE build profiles of people.
Enforcement & Removal Operations (ERO) uses Palantir's ICM to manage and build immigration cases to charge people in court.
They also use the Enforcement Integrated Database (EID) to collect mobile biometric information. Through EID, they share biometric data with the Mexican government. Both EID and the interface for DHS biometric sharing with Mexico are managed by Northern Virginia contractor Dev Technology.
Palantir customized HSI's ICM to interface with ERO's EID.
Palantir ICM
DevTech has cloud-hosting partnerships with AWS.
devtech EID
ICM can collect utilities data, DMV records, real property data, records, business data, healthcare provider information, live cell phone records, and license plate images. HSI uses this data to build profiles of people. It's a large volume of data, and needs to be stored somewhere.That is why all components of ICM are currently being migrated to Amazon Web Services (AWS) GovCloud through a third party.
Palantir FALCON
Immigration agents also use Palantir's FALCON Search and Analysis (FALCON-SA) to identify connections among the different data sets and produce intelligence reports and visuals, such as a web of relationships surrounding a specific person.
DHS agencies store all biometric data in the department's IDENT database (soon to be Northrop Grumman's HART), which contains nearly 230 million unique identities, mostly fngerprint records, as well as 36.5 million face records and 2.8 million irises, with the ability to house palm prints, scars and tattoos
IDENT
IDENT backs up data on the AWS cloud.
NORTHROP GRUMMAN HART
Northrop Grumman is developing the new IDENT database, known as HART, after winning a contract worth more than $94 million through 2021. HART will have greater storage for face and iris, as well as planned options for voice, DNA and other biometric modalities. The system is scheduled to be running by late 2019.
amazon.com
Amazon Web Services (AWS) is Amazon's cloud service that, in all likelihood, will continue to be the primary provider for Department of Homeland Security's services (ICE is just one agency within DHS).
mijente

Amazon at the Top of the "Cloud Industrial Complex"

Amazon has moved from being the one-stop shop for consumers of every kind to the biggest broker of cloud storage space on the planet, through Amazon Web Services. AWS is the primary cloud space where these data-sharing systems live. AWS serves as the key contractor in DHS' migration of the agency's $6.8 billion information technology (IT) portfolio to the cloud. **Amazon, now the wealthiest company on the planet, has more federal authorizations to maintain government data from a variety of government agencies than any other tech company — 204 authorizations, compared to Microsoft's 150, Salesforce's 31, and Google's 27.** It has made wide use of these authorizations, serving as DHS's database for immigration case management systems and biometric data for 230 million unique identities — mostly fingerprint records, alongside 36.5 million face records and 2.8 million irises.



The cloud plays a critical role in the DHS immigration enforcement system. Most key data systems supporting immigration enforcement at DHS are either hosted on commercial cloud providers or being migrated to them. This facilitates massive info-sharing with local, state, and other federal law enforcement agencies, as well as the bilateral info-sharing agreements with countries such as Mexico. **The government's move towards cloud services has been the result of the "cloud industrial complex"— a public-private partnership among industry lobbyists, tech executives, key federal legislators, and tech executives-turned-government officials.**

DHS emerged as a potential treasure trove for Silicon Valley cloud providers in late 2010, when then-Federal Chief Information Officer Vivek Kundra instituted a "Cloud First" policy. The policy encouraged the private contracting of $20 billion in cloud services across the federal government and

projected DHS, specifically, as the largest potential client for cloud service acquisition, at over $2.4 billion.

The federal government's "Cloud First" policy was an important step in constructing what has become a "revolving door" for cloud service providers at the highest levels of government. Congress members involved in a public-private partnership that helped codify the Federal CIO's power in IT acquisition (a role filled by former or future tech executives) have received over $250,000 in contributions from Amazon and other tech companies that then gained these cloud computing contracts.

Within the next couple of years, the entirety of DHS's IT portfolio — full of personally-identifiable data — will live on the cloud. DHS has already granted multi-million dollar cloud contracts to Adobe, Amazon, IBM, Oracle, Salesforce, Zoom, and other Silicon Valley companies. Amazon will likely continue to be the primary provider, which means it is the ultimate keeper of the data that enables detentions and deportations.

Conclusion

We commissioned this report at the onset of the Trump administration, knowing that immigration enforcement would be a centerpiece of their agenda. We know that the fight to #AbolishICE and defend immigrant communities will require action at both the federal and local level. Given our current administration, however, significant change in Washington, D.C., is unlikely. **For true accountability, we must turn to both local political allies and those in the private sector to address the surveillance and tech infrastructure that directly and indirectly facilitate the immigration dragnet.**

It is also clear that policing, detention, and deportation have, indeed, become lucrative enterprises for Silicon Valley companies, and they will only continue to expand without the public scrutiny and proactive measures needed to stop them. And although those solutions are still in the making, we know that there must be multiple tactics and strategies to defend our communities, including:

1. **We call on states, cities, and local municipalities to expand their "sanctuary city" policies by ending: (1) contracts that allow unfettered information sharing technologies and biometric collection to and from ICE; (2) contracts with private data brokers that work with ICE, and (3) predictive policing programs such as those developed by Palantir.** Cities and states that have contracts with Palantir should immediately cancel those contracts. Stopping local law enforcement agencies from collecting, storing, and accessing data on Palantir systems is one important step toward ensuring the civil and human rights of local residents. States should also consider passing strong biometrics privacy protection laws that will allow people to decide how and if their intimate biometric scans should be used.

2. **We call on tech company employees to continue raising their voices against their companies' contracts with military, police, and immigration agencies.** Executives are being put on notice — by the international community, by immigrant rights activists, and by their very own workers. Thousands of tech workers at different firms, from Google to Amazon to Microsoft, have decried their companies' contracts with military and immigration agencies, threatening to withhold their labor if human rights guidelines are not produced to govern the use of tech they themselves created. Tech companies have the means to declare their values and oppose the systems that are jailing immigrants and creating fear within vulnerable communities everywhere.

3. **We call for increased public scrutiny to track Amazon's and Palantir's dominance in meeting the data storage needs of various federal agencies**:
    a. We urge more research profiling both Amazon and Palantir and mapping out the links between them and the various agencies they service.
    b. We call for more detailed analyses of the campaign contributions made by tech lobbyists to federal legislators, the public policy positions of those legislators vis-a-vis cloud computing and other tech contracts, and the "revolving door" of those involved at the highest levels of the tech industry and government.
    c. We beseech all advocates and our movement to develop a fuller understanding of how tech tools, like ICM, work on the ground and what kinds of surveillance and prosecution are enabled by such technology that were not possible before. We can no longer afford to craft and implement anti-immigration enforcement campaigns that ignore the role of tech.

This is not a time to be neutral. As we continue to develop strategies to defend our communities against the Trump/Sessions white supremacist agenda and the human rights crisis it has unleashed, we must challenge everyone in Silicon Valley, from the companies themselves, to their investors, consumers, and workers, to declare which side they are on. Right now, Amazon and Palantir's contracts with DHS plant them firmly on the side of Trump. We must challenge our own movement to understand how the Trump administration in general, and DHS/ICE in particular, finds new ways to target our communities, and to use that information to inform our organizing strategies. We must step up in this unprecedented moment to respond to the threats we face with agility, force and innovation.

Table of Contents

Empower, LLC was commissioned by The Ford Foundation to assist the Gender, Racial and Ethnic Justice thematic area with strategic corporate research to be used as a reference by Mijente, Immigrant Defense Project, and the National Immigration Project of the National Lawyers Guild. Research completed and current through August 23, 2018.

Any additional use or reference to the content of this report should be done so with previous notification of Empower, LLC at the following email address: info@empowerllc.net.

Executive Summary

U.S. Immigration and Customs Enforcement (ICE) has awarded major information technology (IT) contracts to large defense contractors and IT services companies since the agency's inception in 2002. However, changes in policy and contracting have heightened the importance of new technologies and companies in recent years. The two most fundamental changes have been the rapid adoption of cloud services, replacing many key data center functions, and the development of new programs for person-centric case management that are capable of ingesting and analyzing large amounts of personal data. This data includes biometric information, as well as other data sets of personally identifiable information from a wide variety of commercial sources. The emergence of social media has made for one more highly revealing data source.

Meanwhile, ICE and the Department of Homeland Security (DHS) as a whole have expanded their ability to share information with local, state and federal law enforcement agencies, as well as certain foreign governments. The use of these new technologies and sharing capabilities has lengthened the reach of immigration enforcement.

This report identifies a wide range of contractors providing the technological infrastructure that supports federal immigration enforcement and related information sharing. Several companies are of particular strategic importance due to their involvement at multiple points in the profiling, tracking and apprehension of undocumented persons coordinated by ICE and DHS. The overlapping functions of these and other key tech contractors is presented at length in the following report.

COMPANY	HEADQUARTERS	KEY FUNCTION
Amazon.com, Inc. (NASDAQ: AMZN)	Seattle, WA	Cloud hosting for numerous state and federal data systems key to immigration enforcement, including Palantir's Integrated Case Management system at ICE. Amazon Web Services' Justice and Public Safety program sells cloud services to state law enforcement agencies that share information with DHS by various means.
Palantir Technologies, Inc.	Palo Alto, CA	Case management and analysis software for local, regional and federal law enforcement, including key ICE systems and all DHS Fusion Centers in California.
Forensic Logic, Inc.	Walnut Creek, CA	Owner of recently integrated LEAP Network and COPLINK software, the most widely used corporate platform for law enforcement information sharing with DHS, including key regional information sharing agreements in Southwestern border states. Partners with Amazon Web Services' Justice and Public Safety program.

Thomson Reuters Corporation (TSX/NYSE: TRI)	Toronto, Canada *Key subsidiary West Publishing Corp. in Eagan, MN	Data broker with large ICE contracts and interfaces with Palantir and Forensic Logic for the sharing of diverse data sets of personally identifiable information.
IDEMIA France SAS *Majority shareholder is private equity firm Advent International of Boston, MA	Colombes, France *U.S. subsidiary MorphoTrak in Anaheim, CA	Multimodal biometric technology provider for DHS and FBI systems key to immigration enforcement, as well as fingerprint ID systems for some 24 states and an estimated 80 percent market share for REAL ID-compliant cards, in addition to screening the identities of U.S. passport and visa applicants.
NEC Corporation (TYO: 6701)	Tokyo, Japan *U.S. subsidiary NEC Corporation of America in Irving, TX	Provider of mobile biometric devices to ICE, facial recognition technology to CBP, and face and iris matching algorithms to the DHS biometric database, as well as fingerprint ID systems for some 19 states and a multimodal biometric system for the Los Angeles Sheriff's Department, a key regional DHS partner.

Big Data Storage: DHS Data Centers and the Move to the (Amazon) Cloud

Since 2008, DHS has consolidated most functions of 43 agency-specific data centers across the country into two primary data centers in Mississippi and Virginia. DHS is now undergoing an "enterprise-wide migration" of DHS's USD 6.8 billion information technology (IT) portfolio to the cloud. DHS has adopted a "multi-cloud strategy," but many key cloud migrations have been to Amazon Web Services (AWS). Most key data systems supporting immigration enforcement at DHS are either hosted on commercial cloud providers or being migrated to them. This includes ICE's case management tool developed by Palantir, CBP's Biometric Entry-Exit program, DHS's current and future biometric database, and DHS's biometric sharing platform with Mexico.

The Tech Lobby and Revolving Door Behind the Cloud Migration

Adoption of a Cloud First policy was one of the first actions taken by Federal CIO Vivek Kundra in 2010. The policy encouraged the private contracting of USD 20 billion in cloud services across the federal government and projected DHS as the largest potential client for cloud service acquisition, at over USD 2.4 billion. This policy was an important step in constructing what has become a revolving door for cloud service providers at the highest levels of government.

Palantir: A New Foundation for Ice Case Management and Analytics

ICE's two major divisions, Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO), each have their own case management system. The HSI system, known as Integrated Case Management (ICM), is a Palantir product. ICM works in tandem with another Palantir product, FALCON Search and Analysis (FALCON-SA), an analytical tool that helps agents analyze all ingested data, identify connections and produce intelligence reports and visuals. ICM is currently being migrated to AWS.

Meanwhile, the ERO case management system is known as the Enforcement Integrated Database (EID), a repository for mobile biometric collection also used for biometric sharing with the Mexican government. Both EID and the interface for DHS biometric sharing with Mexico are managed by Northern Virginia contractor Dev Technology.

Biometric Data Storage and Sharing: Interoperability on the Cloud

DHS agencies store all biometric data in the department's IDENT database, which backs up data on the AWS cloud. IDENT contains nearly 230 million unique identities, with the ability to house palm prints, scars and tattoos. DHS is currently developing a new, cloud-based biometric system to replace IDENT scheduled to be operational by late 2019, which will have greater storage and matching capabilities, particularly for face and iris, as well as planned options for voice, DNA and other biometric modalities. Northrop Grumman is developing the database, known as HART, after winning a contract worth more than USD 94 million through 2021.

Biometric Sharing with the Mexican Government

DHS has several bilateral agreements in place for biometric information sharing with the Mexican government for purposes of immigration enforcement; in 2017 the DHS signed an agreement with Mexico's National Migration Institute (INM) to regularly source biographic information obtained on "nationals of a third country." Working through the Department of State, the U.S. government commissioned the building of a biometrics system for Mexico's National Migration Institute (INM) in 2017, supporting biometric collection of Central Americans and other individuals being held at detention centers in Mexico.

ICE's Law Enforcement Support Center and FBI Information Sharing

Palantir's ICM system plays a key role in information sharing with law enforcement. ICE agents can access the FBI's National Crime Information Center (NCIC) from within ICM via ICE's Alien Criminal Response Information System (ACRIMe). NCIC contains information from Nlets, a state-owned network of law enforcement agencies that "links together and supports every state, local and federal law enforcement, justice and public safety agency for the purposes of sharing and exchanging critical information," processing some 1.5 billion transactions each year. NCIC is one part of the FBI's Criminal Justice Information Services (CJIS) complex, based in Clarksburg, West Virginia. CJIS also houses other key databases with biometric and personally identifiable information.

DHS Regional Information Sharing Agreements

Palantir's ICM system also shares information directly with local and state law enforcement via ICE's Law Enforcement Information Sharing (LEIS) Service. The most common platform used by local and state law enforcement is COPLINK, used by over 5,100 law enforcement agencies across the country and hosted on the cloud at Nlets in Arizona. COPLINK is currently owned by Northern California company Forensic Logic. Forensic Logic partners with Amazon Web Services as part of AWS's Justice and Public Safety program, in compliance with the FBI's CJIS standards.

A Growing Biometrics Market in U.S. Immigration Enforcement

Contracting with state law enforcement agencies for Automated Fingerprint Identification Systems (AFIS) is effectively split between three companies: Gemalto (Netherlands), NEC Corporation (Japan), and IDEMIA (France).

Iris scanning is playing an increasingly important role in Southwestern border states. In 2017, a Massachusetts-based company called BI2 Technologies agreed to provide its iris scanner system to all 31-member agencies of the Southwestern Border Sheriffs' Coalition. The company collaborates with local law enforcement agencies in 47 states. BI2 received funding in 2015 from TAG Holdings, a company run by John Ashcroft.

1. Introduction

The Department of Homeland Security (DHS), established in 2002 by the second Bush administration in the fallout of the September 11 attacks, claims to "safeguard the American people, our homeland, and our values" and to "secure the nation from the many threats we face."[1] One of those threats, in the eyes of DHS, consists of undocumented persons and irregular immigration. DHS houses seven agencies, of which three are dedicated specifically to the enforcement of immigration laws:

- U.S. Customs and Border Patrol (CBP)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Customs and Immigration Enforcement (ICE)
- Federal Emergency Management Agency (FEMA)
- U.S. Coast Guard (USCG)
- U.S. Secret Service (USSS)
- Transportation Security Administration (TSA)

This report examines the collection and use of biometrics and personally identifiable information for immigration enforcement, and the contracting of new technologies to track and target individuals based on the analysis of massive corporate and governmental data sets. ICE will be the focus of this report, with some emphasis also given to CBP due to its close collaboration and mission overlap in areas of jurisdiction. USCIS is not involved in enforcement operations in the field, but its information systems are largely accessible to ICE and CBP.

The report aims to provide the following:

- An overview of the recent migration of ICE and DHS applications to cloud services, and the role of specific cloud service providers in that migration.
- An overview of IT spending at DHS by agency and by project.

[1] DHS, "About Us," https://www.dhs.gov/about-dhs.

- An overview of the most important person-centric data systems used by ICE and related agencies, and of the private contractors responsible for those systems, including visual representations of how systems communicate and overlap.
- Identification and visuals of the different avenues for ICE and DHS information sharing with local, state and federal law enforcement, as well as international partners, and the private contractors facilitating information sharing.
- Identification of the most common biometric modalities used by ICE and other law enforcement, and the private contractors manufacturing the devices and algorithms that support biometric matching and databases.
- Identification of key data brokers providing information to ICE and to other private contractors involved in case management and analysis, including social media data.

1.1. Sources

The report is based primarily on government and corporate records, including:

- Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) drafted by DHS, the FBI, and other federal agencies.
- International and inter-agency memorandums and information sharing agreements.
- Financial information from the U.S. Government's IT Dashboard, including Business Case documents concerning major IT investments.
- Contracting documents from local, state and federal governments, including information obtained from public records requests (submitted both for this report and by third parties), as well as agency FOIA libraries and federal contracting websites.
- Government statistics regarding cloud adoption and authorization, primarily via FedRAMP.
- Technology testing and standards reports from the National Institute of Standards and Technology (NIST).
- Federal lobbying records from the Lobbying Disclosure Act Database.
- Corporate websites, financial reporting, and informational documents from contractors.
- Incorporation and annual reporting documents from state corporate registries.
- Firsthand information provided by government and corporate leaders, obtained through industry conference video footage; reporting in industry publications; and congressional transcripts.

2. Big Data Storage: From DHS Data Centers to the (Amazon) Cloud

Prior to 2008, the various data systems at DHS agencies were housed at 43 agency-specific data centers around the country. As can be seen in Figure 1, most data centers were located in the capital region, particularly in Virginia and Maryland, but locations ranged from Southern California to Northern Vermont.

Figure 1. DHS data sites prior to data center consolidation

Source: Empower LLC image, data from Senate Appropriations Committee Informational Briefing.[2]

Beginning in 2008, DHS began a data center consolidation process by which it moved most systems to two new facilities: Data Center 1, located in Stennis, Mississippi, on the premises of the National Center for Critical Information Processing and Storage within the NASA Stennis Space Center; and Data Center 2, in Clarksville, Virginia, close to the North Carolina border. The Mississippi facility was first operated by the company CSC Government Solutions (now CSRA, owned by General Dynamics), while the Virginia facility was operated by HP Enterprise Services (now DXC Technology, the result of a merger between HP Enterprise Services and CSC, the former parent company of CSC Government Solutions, in 2015). Both companies have been awarded contracts for hundreds of millions of dollars for this work.[3]

CBP still maintains a data center in Springfield, Virginia, and Irish company Accenture won a contract worth over USD 300 million in 2017 for CBP data center services at that location and Data Centers 1 and

[2] DHS Data Center Migration Overview, August 2011, released in response to FOIA request, accessible at assets.fiercemarkets.net/public/sites/govit/dhs_foia_datacenters.pdf.

[3] Data Center 1 contracts include HSHQDC08J00169 and HSHQDC16D00001; Data Center 2 contracts include HSHQDC07J00515 and HSHQDC15D00015.

2.[4] (Accenture was also awarded a five-year, USD 297 million contract in 2017 to undertake the hiring of some 7,500 new CBP agents at the behest of the Trump administration.[5])

Figure 2. DHS Data Centers 1 and 2

Source: Empower LLC image, data from DHS, "Data Centers," https://www.dhs.gov/data-centers.

The data center consolidation at DHS began even before the roll-out of the Obama administration's Federal Data Center Consolidation Initiative in 2010, and the DHS CIO at the time, Richard Spires, played an important role in that program.[6] But just as the two new DHS data centers were getting off the ground, a new IT phenomenon was taking shape in Washington: the advent of cloud computing services. Cloud computing was alluded to in plans for data center consolidation but soon became a policy priority in itself with the announcement in late 2010 of a "Cloud First" policy by Federal CIO Vivek Kundra.

The Cloud First policy characterized federal IT practices as "de-coupled from private sector innovation engines" and claimed that "cloud computing offers the government an opportunity to be more efficient, agile, and innovative through more effective use of IT investments, and by applying innovations developed in the private sector." The report estimated that USD 20 billion of the federal government's USD 80 billion annual IT budget at the time could be re-directed to cloud computing services. Of all federal agencies, it estimated that DHS had the greatest potential for cloud service acquisition, at over USD 2.4 billion. "By

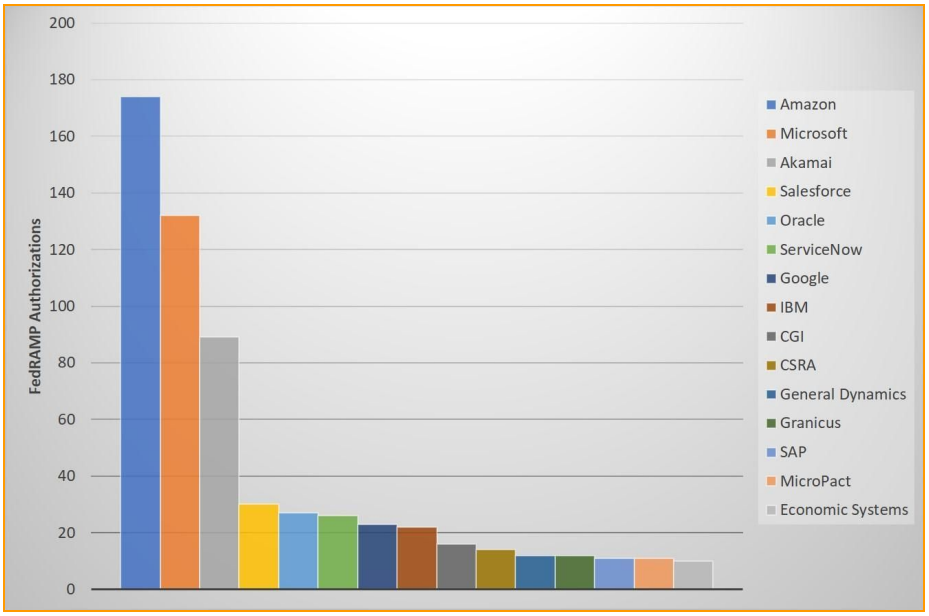
[4] Award ID HSBP1017C00137, https://www.usaspending.gov/#/award/23782745.
[5] Award ID 70B06C18D00000001, https://www.usaspending.gov/#/award/8287770. See also: Ross Wilkers, "Accenture wins $297M Border Patrol agent hiring support contract," Washington Technology, December 18, 2017, https://washingtontechnology.com/articles/2017/12/18/accenture-cbp-hiring-contract.aspx.
[6] DHS, "Federal Data Center Consolidation Initiative 2011 Data Center Consolidation Plan & Progress Report," October 2011, https://www.dhs.gov/sites/default/files/publications/DHS_FDCCI_Report_Oct_2011_Final508.pdf

leveraging shared infrastructure and economies of scale," the policy reads, "cloud computing presents Federal leadership with a compelling business model."[7]

More concretely, it was cloud service providers such as AWS that had presented the federal government with a compelling business model, and which have seen colossal benefits from the Cloud First policy. Amazon, currently on pace to become one of the world's first companies with a valuation of more than USD 1 trillion, has seen its cloud division become its most powerful driver of growth, with quarterly revenues of over USD 6 billion in Amazon's most recent earnings report. AWS dominates the cloud services market, with an estimated 34% worldwide market share, more than its next four competitors—Microsoft (14%), IBM (8%), Google (6%) and Alibaba (4%)—combined.[8] Amazon occupies an outsized role in U.S. government cloud services. The company has a USD 600 million for comprehensive cloud services with the CIA and is favored to win a cloud contract with the Department of Defense worth up to USD 10 billion.[9]

Cloud services for the federal government are dominated by Amazon and Microsoft, which have the largest number of FedRAMP authorizations across federal agencies.

Figure 3. Cloud Service Providers with 10 or more FedRAMP authorizations



Source: Empower LLC image, data from FedRAMP Marketplace, https://marketplace.fedramp.gov/#/products?sort=productName.

[7] Federal CIO Vivek Kundra, "Federal Cloud Computing Strategy," February 8, 2011, https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf.
[8] Mike Robuck, "Amazon Web Services is in a league of its own for cloud revenue, report says," Fierce Telecom, July 30, 2018, https://www.fiercetelecom.com/telecom/amazon-web-services-a-league-its-own-for-cloud-revenue-report; James Bourne, "AWS revenues go up 49% year on year, remains 'in a league of its own'," CloudTech, July 30, 2018, https://www.cloudcomputing-news.net/news/2018/jul/30/aws-revenues-go-49-year-year-remains-league-its-own/.
[9] Naomi Nix, Ben Brody, and Kathleen Miller, "Pentagon's Winner-Take-All Move on Cloud Contract Expected to Favor Amazon," Bloomberg, July 26, 2018, https://www.bloomberg.com/news/articles/2018-07-26/pentagon-goes-with-winner-take-all-10-billion-cloud-contract.

DHS was an early adopter of Amazon cloud services, beginning with USCIS. The agency's CIO from 2010 to 2017, Mark Schwartz, was a devoted advocate of cloud migration, and he oversaw the migration of the core USCIS data systems to Amazon Web Services.[10] In 2017, Schwartz left DHS to work as Enterprise Strategist at Amazon Web Services, having essentially handed an entire government agency over to the company for cloud hosting.[11]

In May 2018, DHS CIO John Zangardi noted that 29 applications at DHS headquarters had been migrated to cloud services, and another 70 had been identified for migration, as part of a "multi-cloud strategy" using multiple providers.[12] "Different [DHS] components have different needs," according to Zangardi. "We don't want a hundred cloud [providers], but this will be a hybrid strategy that will allow for multiple players."[13] Zangardi further explained, "Some components have been very aggressive in moving out there. Immigration and Citizenship Enforcement and Customs and Border Protection have done a fantastic job. There are smaller components and other components that need help."[14] In other words, the three immigration-related agencies at DHS are at the forefront of DHS cloud migration.

Zangardi recently appointed a cloud steering group, headed by DHS Under Secretary for Management Claire Grady. DHS has a Cloud Action Officer and Deputy Director of Mission and Strategy, Kshemendra Paul, who works on behalf of Zangardi and Grady. Paul's LinkedIn profile describes his position as "leading efforts to organize, accelerate, and optimize the enterprise-wide migration of DHS' ~$6.8B IT Portfolio to the Cloud, and to optimize our remaining data centers."[15] In keeping with figures cited later in this report, USD 6.8 billion represents the entirety of the DHS IT budget. "We're already in the cloud," Paul said. "There are early adopters across the department. We've overcome barriers and the migration is well underway."[16]

It is difficult to quantify the extent to which DHS agencies have moved data systems to particular commercial cloud services, as the agencies do not generally sign contracts with the providers themselves but with third-party contractors, not all of which name the cloud service providers to be used. However, public records of the contracts signed with these third parties reveal that, in keeping with CIO Zangardi's comments on CBP and ICE, most key data systems supporting immigration enforcement at DHS are either hosted on commercial cloud providers or being migrated to them:

---

[10] Derek Major, "How USCIS went agile and open to move application process online," GCN, October 29, 2015, https://gcn.com/articles/2015/10/29/uscis-agile-forms.aspx?m=1; Steven Nelson, "Amazon spotlights work with federal immigration agency," Washington Examiner, June 21, 2018, https://www.washingtonexaminer.com/news/white-house/amazon-spotlights-work-with-federal-immigration-agency.

[11] Mark Schwartz LinkedIn profile, https://www.linkedin.com/in/innovativecio/.

[12] Nick Wakeman, "DHS CIO plans multi-cloud strategy," FCW, May 29, 2018, https://federalnewsradio.com/federal-cloud-report/2018/07/senate-praises-dhs-data-center-consolidation-effort-by-opening-up-its-wallet-for-2019/.

[13] Phil Goldstein, "DHS Sees Many Benefits in Cloud Migration," FedTech, June 28, 2018, https://fedtechmagazine.com/article/2018/06/dhs-sees-many-benefits-cloud-migration.

[14] Nick Wakeman, "DHS CIO plans multi-cloud strategy," FCW, May 29, 2018, https://federalnewsradio.com/federal-cloud-report/2018/07/senate-praises-dhs-data-center-consolidation-effort-by-opening-up-its-wallet-for-2019/.

[15] Kshemendra Paul LinkedIn profile, https://www.linkedin.com/in/kshemendrapaul.

[16] MeriTalk, "DHS Official: Cloud Business Value Still Developing, but MGT Key," June 6, 2018, https://www.meritalk.com/articles/dhs-official-cloud-business-value-still-developing-but-mgt-key/.

- The core application processes at USCIS are all hosted on Amazon cloud services.[17]
- ICE's two current major IT investments—including the Integrated Case Management software, HSI's "core law enforcement case management tool," designed by Palantir—are being migrated in their entirety to Amazon cloud services.[18]
- CBP put out a request for proposals in February 2018 to migrate all CBP applications out of the CBP data center in Springfield, Virginia, to commercial cloud service providers by September 2019.[19]
- CBP's Biometric Entry-Exit program is already at least partially hosted on AWS.[20]
- The DHS biometric database, IDENT, is backed up on the Amazon cloud,[21] and its replacement, currently in development by Northrop Grumman, will be cloud-based.
- The DHS platform for biometric sharing with Mexico, being developed by DHS contractors in cooperation with the Department of State, is a cloud-based application hosted by an undisclosed provider.[22] Dev Technology, the company contracted to build the application, has cloud-hosting partnerships with AWS and Microsoft Azure.[23]

Within the next couple of years, most DHS systems will live on the cloud, and in all likelihood AWS will continue to be the primary provider. As seen in Figure 4, AWS has three data centers in Northern California and three in Oregon (AWS West), as well as three in Ohio and six in Northern Virginia (AWS East). AWS GovCloud, designed specifically for government services—though federal agencies also use AWS West and AWS East—is run at three data centers at an undisclosed location on the West Coast. The company is also in the process of opening up a second cluster of GovCloud services in the eastern United States.

---

[17] Derek Major, "How USCIS went agile and open to move application process online," GCN, October 29, 2015, https://gcn.com/articles/2015/10/29/uscis-agile-forms.aspx?m=1; Steven Nelson, "Amazon spotlights work with federal immigration agency," Washington Examiner, June 21, 2018, https://www.washingtonexaminer.com/news/white-house/amazon-spotlights-work-with-federal-immigration-agency.

[18] For migration of Palantir's ICM, see Award ID HSCETE16J00343, https://www.usaspending.gov/#/award/23850509. See also: DHS, ICE Office of Acquisition Management, Limited Source Justification for Award ID HSCETC13F00035, May 15, 2018, https://govtribe.com/project/tecs-mod-leiss-and-data-migration, and DHS, ICE Office of Acquisition Management, Limited Source Justification for Award ID HSCETC14F00041, May 15, 2018, https://govtribe.com/project/tecs-mod-tech-assistance. For migration of SEVIS components, see: Development Consultants Inc., "U.S. Department of Homeland Security (DHS) Student and Exchange Visitor Program (SEVP) Case Study," https://www.devconinc.com/dci/case-study-student-and-exchange-visitor-program/.

[19] CBP, Cloud Acquisition RFP, Solicitation No. CBPRFI20180228, https://www.fbo.gov/index?s=opportunity&mode=form&id=2e17c841b333de39740363f71813aa62&tab=core&_cview=0 (CBP migration).

[20] Award ID HSBP1017J00789, https://www.usaspending.gov/#/award/23783978. See also: CBP Biometric Entry-Exit Business Case, U.S. Government IT Dashboard, https://itdashboard.gov/drupal/reports/business-case-pdfs.

[21] See Award ID HSHQDC16J00145 for reference to IDENT data back-up, https://www.usaspending.gov/#/award/24243314.

[22] Dev Technology Group, "Services We Provide," devtechnology.com/new/wp-content/uploads/2018/06/Dev-Technology-Capabilties-2018-02.pdf,devtechnology.com/new/wp-content/uploads/2018/06/Dev-Technology-Capabilties-2018-02.pdf. See also: Award ID 19MX9018C0002, https://www.usaspending.gov/#/award/5845750; and Award ID 70B04C18F00000490, https://www.usaspending.gov/#/award/67072955.

[23] Dev Technology, Services, devtechnology.com/service/.

Figure 4. Location of U.S. Amazon Web Services data centers, excluding GovCloud

Source: Empower LLC image, data from AWS, Global Infrastructure, https://aws.amazon.com/about-aws/global-infrastructure/.

Microsoft Azure data centers in the United States are less centralized, with two facilities in Virginia and one each in Iowa, Illinois, Texas, Wyoming, Washington and California.[24]

Across the federal government, there are currently some 111 cloud providers authorized under FedRAMP, 71 in process, and 19 in early application stages.[25] Of these companies, 22 have authorization with DHS. The information in Table 1, provided by the federal government, is incomplete as some DHS agencies using AWS are not mentioned. For example, all core USCIS systems use AWS and key ICE systems are being moved onto AWS. Amazon is the cloud host most frequently mentioned in third-party IT contracts with DHS, through companies including JHC Technology[26] and Aquilent[27] (USCIS); Four Points Technology[28] (CBP and ICE) and GovPlace (DHS Office of Procurement Operations).[29] DHS Procurement Operations also has a contract with Blackstone Technology Group, which partners with cloud hosts Microsoft and Oracle for cloud migration services,[30] and Microsoft has its own "indefinite

[24] Microsoft, Azure locations, https://azure.microsoft.com/en-us/global-infrastructure/locations/.

[25] FedRAMP Marketplace, https://marketplace.fedramp.gov/#/products?sort=productName.

[26] DHS Award ID HSSCCG17F00258, https://www.usaspending.gov/#/award/24268217.

[27] DHS Award ID HSSCCG16F00362, https://www.usaspending.gov/#/award/24267408.

[28] DHS Award ID HSBP1017J00789, https://www.usaspending.gov/#/award/23783978; DHS Award ID 70CMSD18FR0000022, https://www.usaspending.gov/#/award/62522780; DHS Award ID HSBP1016J00976, https://www.usaspending.gov/#/award/23781670.

[29] Search terms "Amazon" and "AWS" on www.usaspending.gov return considerably more DHS contracts for cloud hosting via third parties than Microsoft or other cloud service providers.

[30] DHS Award ID HSHQDC14J00341, https://www.usaspending.gov/#/award/24241456.

delivery/indefinite quantity" (IDIQ) contract with DHS for services including cloud migration through 2020.[31]

Table 1. Cloud service providers with DHS FedRAMP authorization

Cloud Service Provider	Cloud Service Offering	Subagency
Adobe	Adobe Experience Manager Managed Services (AEMMS-EW)	United States Citizenship and Immigration Services
Akamai	Content Delivery Services	
Amazon	AWS GovCloud	Federal Law Enforcement Training Centers
Amazon	AWS GovCloud	Federal Emergency Management Agency
Amazon	AWS US East/West	Customs and Border Protection
CGI Federal (5 records)	CGI IaaS Cloud	
CGI Federal	CGI IaaS Cloud	Immigration and Customs Enforcement
CoSo Cloud, LLC	CoSo Cloud FedRAMP Managed Service Platform	
CoSo Cloud, LLC	CoSo Cloud FedRAMP Managed Service Platform	Transportation Security Administration
DXC Technology	DXC Cloud for Public Sector	
Economic Systems (2 records)	Economic Systems Federal Human Resources Navigator	
Gordian	Gordian Federal Cloud powered by RSMeans Data	
IBM	IBM Maximo and TRIRIGA	
IBM	SmartCloud for Government	Federal Law Enforcement Training Centers
Knight Point Systems	CloudSeed	
MicroFocus	Fortify on Demand	
MicroPact	MicroPact Product Suite	Customs and Border Protection
Microsoft	Office 365 Multi-Tenant & Supporting Services	
Oracle	IaaS/PaaS - US Government Cloud	

[31] DHS, Microsoft Enterprise Services IDIQ, https://www.dhs.gov/microsoft-enterprise-services-idiq.

Oracle	Oracle Service Cloud	Customs and Border Protection
Rackspace Government Solutions	Federal Community Cloud Platform	United States Coast Guard
Salesforce	Salesforce Government Cloud	United States Citizenship and Immigration Services
ServiceNow	ServiceNow Service Automation Government Cloud Suite	United States Citizenship and Immigration Services
Softlayer	Softlayer Federal Cloud (SFC)	United States Citizenship and Immigration Services
Softlayer	Softlayer Federal Cloud (SFC)	Federal Law Enforcement Training Centers
Zimperium	Zimperium Federal Cloud	
Zoom Video Communications, LLC	Zoom for Government	
Collibra	Data Governance Center	
Lookout, Inc.	Lookout Mobile Endpoint Security	

Source: FedRAMP, DHS Products Used, https://marketplace.fedramp.gov/#/agency/department-of-homeland-security?sort=name.

2.1. The Tech Lobby and Revolving Door Behind the Cloud Migration

The Office of Electronic Government and Information Technology was established in 2002, the same year as DHS. Its first Administrator was a former Unisys and IBM executive, but under the Obama administration the post came to be known as Federal CIO and became an even more active revolving door, specifically for major cloud service providers:

- The first Federal CIO and author of the Cloud First policy, Vivek Kundra, left the office in 2011 to take a job at Salesforce a year later.[32]
- The second Federal CIO, Steven Roekel, worked at Microsoft from 1994 to 2009.[33]
- The third Federal CIO, Tony Scott, was CIO of Microsoft from 2008 to 2013 and CIO of cloud provider VMware from 2013 until his 2015 federal appointment.[34]

[32] Vivek Kundra, LinkedIn profile, https://www.linkedin.com/in/vivekkundra/.

[33] Obama White House, "President Obama Announces More Key Administration Posts," August 4, 2011, https://obamawhitehouse.archives.gov/the-press-office/2011/08/04/president-obama-announces-more-key-administration-posts.

[34] Tony Scott LinkedIn profile, https://www.linkedin.com/in/tony-scott-9ab2172a/.

Microsoft and Salesforce have the second- and fourth-largest number of FedRAMP authorizations among all commercial cloud providers. VMware, now owned by Dell EMC, is also an authorized FedRAMP cloud service provider at multiple federal agencies.[35]

In August 2016, Federal CIO and former Microsoft CIO Tony Scott issued a development freeze on data centers, prohibiting agencies from budgeting "any funds or resources toward initiating a new data center or significantly expanding an existing data center" without special permission from the CIO's office, based on extensive justification.[36] In keeping with the Cloud First policy, the initiative emphasized that cloud investment should be the priority for all federal agencies, whether for Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).

While such direct language effectively calling for the handover of federal IT services to Amazon, Microsoft and other cloud service providers had not been codified into law, the basis for such directives were established in the 2014 Federal Information Technology Acquisition Reform Act (FITARA). Broadly speaking, FITARA did two things: it expanded the powers of CIOs in federal agencies with regard to budgeting and IT acquisitions, and it called for data center consolidation and cost savings in federal IT operations, with quarterly reporting obligations.[37]

While the two initiatives might appear to seek a mere streamlining of IT acquisition and oversight, there was a more concrete intent behind them. As mentioned above, CIOs in federal government are often former or future tech industry executives, and codifying their power in IT acquisition decision-making strengthened industry influence over the contracting of its own services. The consolidation and cost savings mandates are a clear, if veiled, reference to commercial cloud services; the Cloud First policy claims that "by using the cloud computing model for IT services, we will be able to reduce our data center infrastructure expenditure by approximately 30%."[38] FITARA does not address cloud computing in any detail, but mandates that data center consolidation shall be "consistent with Federal guidelines on cloud computing security," specifically FedRAMP, which oversees authorization processes for federal cloud service providers, and the National Institute of Standards and Technology (NIST).

The original FITARA House legislation was sponsored by Darrell Issa (R-CA) and Gerald Connolly (D-VA). In January 2014, as they were trying to move FITARA through Congress, Issa and Connolly announced the formation of two groups: the Cloud Computing Caucus and the Cloud Computing Caucus Advisory Group.[39] The former was a congressional caucus and the latter a lobbying group founded by Amazon, Microsoft and EMC (now Dell EMC). In essence, Issa and Connolly announced the formation of a public-private congressional committee.

---

[35] FedRAMP Marketplace, https://marketplace.fedramp.gov/#/products?status=Compliant&sort=productName.

[36] Federal CIO Tony Scott, Memorandum for Heads of Executive Departments and Agencies, August 1, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_19_1.pdf

[37] H.R.1232 — 113th Congress (2013-2014), https://www.congress.gov/bill/113th-congress/house-bill/1232.

[38] Federal CIO Vivek Kundra, "Federal Cloud Computing Strategy," February 8, 2011, https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf.

[39] Kenneth Corbin, "Is the Federal Government Ready to Embrace the Cloud?" CIO, January 16, 2014, https://www.cio.com/article/2379539/government-use-of-it/is-the-federal-government-ready-to-embrace-the-cloud-.html.

Representing a district in Northern Virginia, Connolly comes from a high-tech corridor that houses many IT contractor facilities. Between the two of them, Issa and Connolly have received at least USD 151,000 in direct campaign contributions from the three companies' PACs, without including soft money donations or the numerous contributions from other cloud providers and tech companies. Including the other six current members of the Cloud Computing Caucus Advisory Group, the number of direct contributions from the three companies' PACs alone rises to over a quarter-million dollars.[40]

The Cloud Computing Caucus Advisory Group is a subsidiary of the non-profit Government Technology Alliance, which is headed by President Stephen O'Keeffe,[41] who announced the formation of the Cloud Computing Caucus and its tech industry counterpart in January 2014 alongside Representatives Issa and Connolly. O'Keeffe organizes several tech industry groups through his firm MeriTalk, a subsidiary of holding company 300Brand, Inc., of which O'Keeffe is founder and principal.[42] O'Keeffe regularly organizes industry events with CIOs from across the federal government. In June 2018, O'Keeffe hosted DHS CIO John Zangardi and Cloud Action Officer Kshemendra Paul at a MeriTalk forum where the two spoke about the importance of the MGT Act, signed into law by Donald Trump in December 2017 and co-authored by Will Hurd (R-TX) and Gerry Connolly, and co-sponsored by Connolly's fellow members of the Cloud Computing Caucus Advising Group including Darrell Issa, Ted Lieu and Barbara Comstock, as well as former Microsoft executive Suzan DelBene (D-WA). The MGT Act provides working capital for IT modernization efforts including the acceleration of cloud computing acquisitions.[43]

Many companies have lobbied for FITARA, as can be seen in Table 2. Unsurprisingly, most of the same companies are currently authorized under FedRAMP to provide cloud services to federal government agencies, and the others are almost all service providers that have business partnerships with FedRAMP-authorized cloud providers. In addition to these companies, industry associations including the Information Technology Industry Council, the Business Software Alliance, and the Internet Association—all led and funded by many of the same companies—also lobbied for FITARA, as did the U.S. Chamber of Commerce.[44]

Table 2. FedRAMP authorization of companies that lobbied for FITARA

Company	No. of FedRAMP authorizations	DHS FedRAMP authorization
Accenture	3	No
Adobe Systems	9	Yes
Amazon	174	Yes

[40] Federal Election Commission receipt data; see annexed spreadsheet "Cloud contributions." Other Cloud Computing Caucus Advisory Group members include Ted Lieu (D-CA), Barbara Comstock (R-MA), Tony Cardenas (D-CA), Mark Walker (R-CA), Paul Gosar (R-AZ) and Hank Johnson (D-GA). See: www.cloudcomputingcaucus.org/about/.

[41] Government Technology Alliance 2016 Form 990.

[42] Stephen O'Keeffe biography, FITARA Forum, www.fitaraforum.com/speaker/steve-okeeffe/.

[43] H.R.2227 — 115th Congress (2017-2018), https://www.congress.gov/bill/115th-congress/house-bill/2227/text.

[44] Lobbying Disclosure Act Database, https://soprweb.senate.gov/index.cfm?event=selectfields.

Microsoft	132	Yes
Dell Technologies	3 (VMware)	No
Deloitte	2	No
NetApp	0 (Major CSP partner)	No
EMC	3 (VMware)	No
IBM	22	Yes
VMware	3	No
Lockheed Martin	0	No
Oracle	27	Yes
SAP	11	No
Symantec	1	No
SAIC	1	No
Red Hat	0 (Major CSP partner)	No
NIC	0	No
Panasonic	0	No
Compuware	0 (Major CSP partner)	No
Tanium	0 (Major CSP partner)	No
NTT Data Federal	0 (Major CSP partner)	No
Salesforce	30	Yes
BMC	2	No
Iron Mountain	0 (Major CSP partner)	No
Blackberry	5	No
CA	0 (In process)	No
Autodesk	0 (Major CSP partner)	No
Flexera Software	0	No

Source: Lobbying Disclosure Act Database; FedRAMP.

We begin with this look into the rapidly growing importance of government cloud services because federal agency IT budgets do not always convey the magnitude and importance of the move to the cloud.

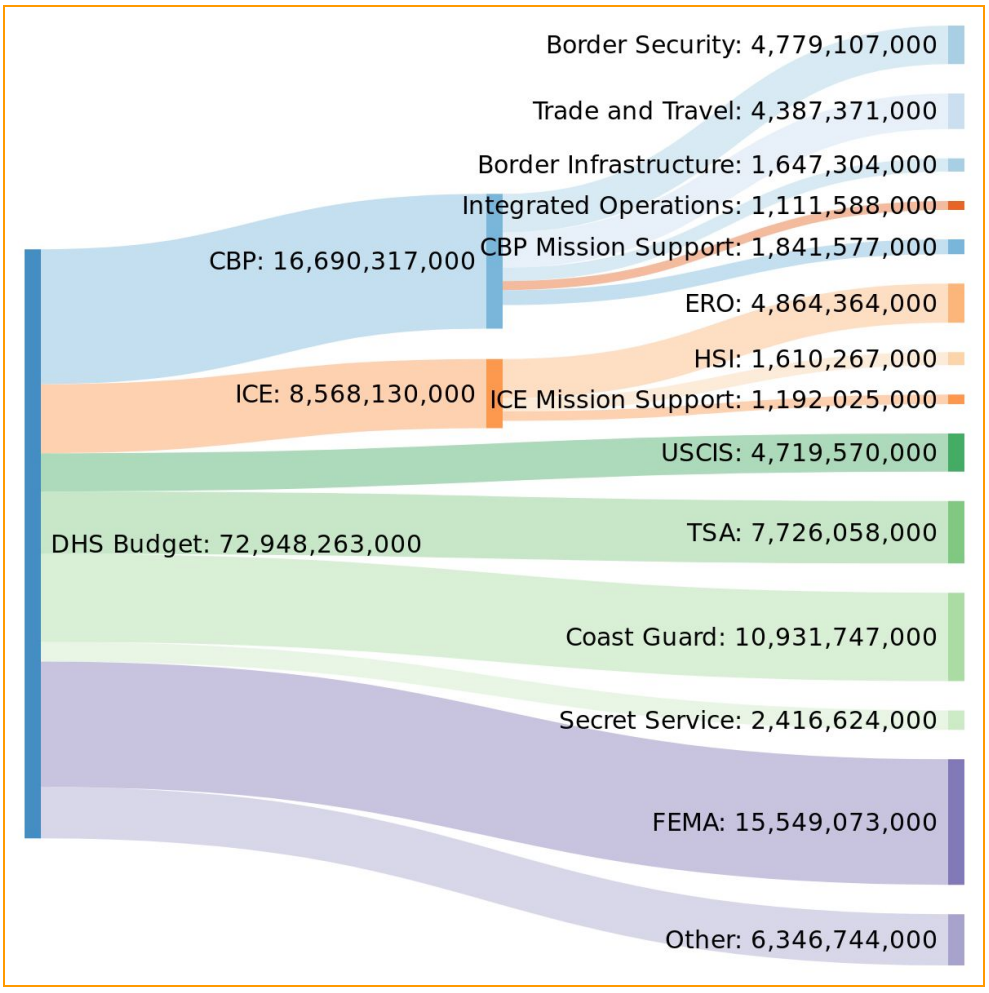
However, reading the fine print of contracting documents and IT project outlines, their importance comes into focus, as seen in the following section.

3. Federal Data Systems for Person-centric Immigration Enforcement

3.1. IT Spending at DHS

The three immigration-specific agencies within DHS account for 41% of total DHS funding requested for congressional approval in the 2019 President's budget. Figure 5 further breaks down CBP and ICE into primary areas of spending.

Figure 5. President's FY 2019 DHS Budget requested spending

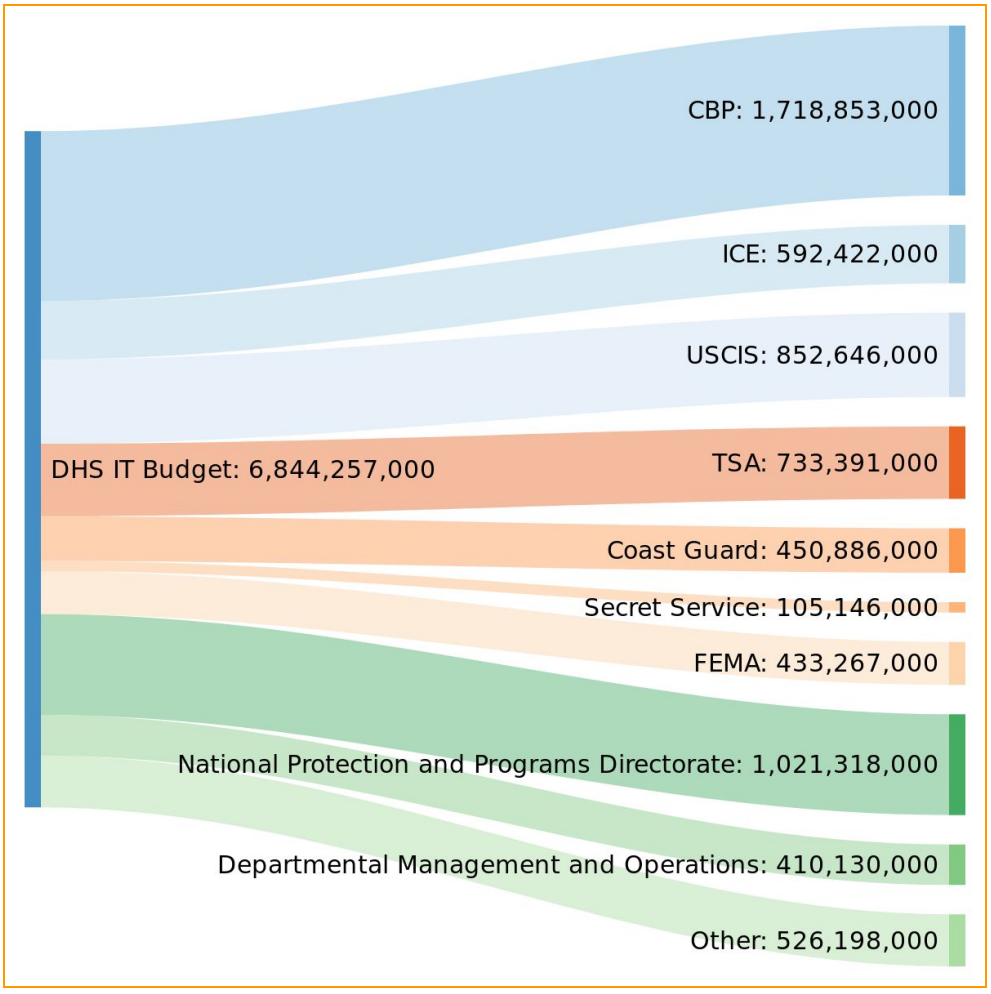


Source: Empower LLC image, data from DHS Congressional Budget Justification FY 2019.

As can be seen in Figure 6, IT spending accounts for USD 6.8 billion, or 9.4%, of the projected DHS budget. As a percentage, this is the largest departmental IT budget in the federal government, with the exception of the much smaller Department of the Treasury (23.9%). As a dollar amount, it is the largest IT budget with the exception of the much larger Department of Defense (USD 29.4 billion).[45]

CBP, USCIS and ICE account for a disproportionate 42.6% of IT spending at DHS, and the figure is actually higher considering that another 28.6% of the IT budget is dedicated to department-wide projects and programs.

Figure 6. President's FY 2019 DHS Budget, IT spending



Source: Empower LLC image, data from U.S. Government IT Dashboard.

While each agency has its own databases and applications, DHS IT is often funded and organized on a department-wide basis. For example, the Office of Biometric Identity Management (OBIM)—the repository

[45] Calculations based on federal agencies' proposed FY 2019 budgets and U.S. Government IT Dashboard, https://itdashboard.gov/drupal/.

for biometric information collected by all DHS agencies—is part of the National Protection and Programs Directorate, which is the second-largest recipient of IT funding after CBP. The development of data systems are generally multi-year projects that arise as needed, and so contracting of IT services, while accounted for in piecemeal fashion in annual budgets, is sometimes organized on an "indefinite delivery/indefinite quantity" (IDIQ) basis. Currently, DHS uses a department-wide contracting vehicle known as EAGLE II (Enterprise Acquisition Gateway for Leading-Edge Solutions II), which was initiated in 2010 but for which major contracting began in 2013.

Through the second quarter of FY 2018, total EAGLE II contracting had reached USD 5.48 billion, of which USD 1.49 billion came in the preceding year. This amounts to approximately 21.9% of IT spending during the same period,[46] meaning that most IT spending at DHS takes place outside of the EAGLE II contracting vehicle. Nonetheless, the contractors in Tables 3 and 4 have been some of the most important service providers at ICE and CBP over the last several years, as EAGLE II provides the flexibility to hire designated contractors on a recurring basis as needed. Tables 3 and 4 include figures for ICE and CBP contracts only, and do not include figures for contracts procured by the same companies outside the scope of EAGLE II.

Table 3. EAGLE II service providers for ICE, contract totals over USD 20 million

ICE Contractor	ICE contract totals w/ all options (USD)
DEV TECHNOLOGY GROUP, INC.	119,645,117
KNIGHT POINT SYSTEMS, LLC	82,954,831
STRATEGIC ENTERPRISE SOLUTIONS, INC.	62,070,738
360 IT INTEGRATED SOLUTIONS	30,999,861

Source: DHS EAGLE II Metrics, FY 2018 Q2 (totals since 2013).

Table 4. EAGLE II service providers for CBP, contract totals over USD 20 million

CBP Contractor	CBP contract totals w/ all options (USD)
UNISYS CORPORATION	441,400,176
MANTECH ADVANCED SYSTEMS INTERNATIONAL, INC.	229,045,224
NTT DATA FEDERAL SERVICES, INC	104,622,648
DELOITTE CONSULTING LLP	103,212,464
CAMBRIDGE INTERNATIONAL SYSTEMS INC.	36,175,974
VIATECH SYSTEMS, INC.	35,600,635
L-3 NATIONAL SECURITY SOLUTIONS, INC.	34,510,187
DEV TECHNOLOGY GROUP, INC.	27,679,614

[46] Calculations based on EAGLE II metrics and budget data from the U.S. Government IT Dashboard.

360 IT INTEGRATED SOLUTIONS	20,738,648

Source: DHS EAGLE II Metrics, FY 2018 Q2 (totals since 2013).

Tables 3 and 4 identify some of the more regular IT contractors for ICE and CBP, but to undertake a more targeted analysis of the major contractors that develop and host person-centric data systems to aid in civil and criminal immigration cases, it will help to first map out those systems.

Of the USD 6.8 billion that DHS has budgeted for FY 2019, funding is split between "major investments" (USD 2.1 billion) and "non-major investments" (USD 4.7 billion). Of some 380 active investments, 39 are classified as major. Of these, two pertain to ICE investments, twelve to CBP investments and two to USCIS investments, in addition to six department-wide investments. These investments do not correspond to all key data systems at each agency, but they do highlight funding priorities in the rapidly-changing IT landscape. Table 5 provides a list of major IT investments at DHS relating to person-centric immigration enforcement and border infrastructure. Most of the following investments involve multiple contractors.

Table 5. Major IT Investments at DHS (person-centric immigration enforcement)

Investment	FY 2019 total (mm USD)	FY 2019 cloud (mm USD)	Cost through 2019 (mm USD)	Description	Principal contractor (Parent company)
ICE - TECS Modernization	24.614	6.296	259.182	The ICE TECS Modernization program will allow ICE to migrate away from using the legacy TECS system, which is managed by CBP, to a modern investigative case management solution.	Palantir; Amazon cloud hosting contract with Four Points Technology
ICE - Student and Exchange Visitor Information System (SEVIS)	45.722	0.36	466.448	SEVIS is a web-based system that tracks information on non-immigrant students, exchange visitors, and dependents who are in the US on F, M, or J classes of admission during approved participation at a US educational institution or exchange visitor program.	Wexler Technical Solutions; Amazon cloud services used [47]
CBP - Biometric Entry-Exit	97.22	4.315	260.39	The Biometric Entry-Exit investment will provide a biometric matching service that will provide CBP the capability to biometrically confirm the arrival to and departure from the United States for all	Unisys; Amazon cloud hosting contract with Four Points Technology

[47] Development Consultants Inc., "U.S. Department of Homeland Security (DHS) Student and Exchange Visitor Program (SEVP) Case Study," https://www.devconinc.com/dci/case-study-student-and-exchange-visitor-program/.

				in-scope travelers at air, land, and sea ports.	
CBP - TECS Modernization	50.01	0	544.487	TECS Modernization is a CBP Business case to modernize TECS' subject record "watch list" processing and Primary and Secondary inspection support at Ports of Entry. Other applications provide for examination of travel documents and encounter data.	Northrop Grumman
CBP - Land Border Integration	74.141	0	1,233.409	LBI maintains/supports WHTI technology developed for inbound vehicles and the capabilities reused in other mission areas: pedestrian inbound, vehicle outbound, U.S. Border Patrol checkpoints and integrates/shares systems and data across these missions.	Unisys
CBP - Integrated Fixed Towers	24.936	0	339.427	Integrated Fixed Towers (IFT) is a system that provides automated, persistent wide area surveillance for the detection, tracking, identification, and classification of illegal entries.	EFW Inc. (Elbit Systems Ltd.)
CBP - Remote Video Surveillance System (RVSS) Upgrade Program	72.503	0	415.045	RVSS systems consist of day and night cameras attached to fixed towers which allows the Border Patrol to monitor border activity through video transmissions to a control room.	General Dynamics One Source LLC (General Dynamics)
CBP - Arrival and Departure Information System (ADIS)	29.24	0	235.056	ADIS is an electronic system that collects biographic information about non-U.S. citizens who travel to the U.S., including arrival, departure, and current immigration status.	Northrop Grumman
NPPD - Automated Biometric Identification System (IDENT)	11.883	0	970.405	As of June 2017, IDENT stores over 215 million separate and distinct identities. The fingerprint gallery currently grows at a rate of approximately 2 million fingerprint records a month.	CSRA (General Dynamics); system backs up data on the Amazon Web Services cloud[48]

[48] See Award ID HSHQDC16J00145 for reference to IDENT data back-up, https://www.usaspending.gov/#/award/24243314.

NPPD - Homeland Advanced Recognition Technology (HART)	168.808	0	571.846	OBIM is the lead entity within DHS responsible for biometric identity management services. OBIM is in the acquisition and development stage of HART as a replacement for IDENT.	Northrop Grumman; HART is a cloud-based system

Source: U.S. Government IT Dashboard and IT Business Case documents.

As can be seen above in Table 5, the two ICE systems receiving the most IT funding are hosted on Amazon cloud services, and key new biometric systems are also cloud-based. It should be noted that some systems using cloud services do not report cloud-specific funding for FY 2019, meaning that cloud migration at DHS is more widespread than IT budget figures would indicate. Of DHS's USD 6.8 billion IT budget for FY 2019, USD 141.62 million (or just 0.2%) is budgeted for cloud services.

The focus of this report is on person-centric data systems, particularly those that aid in the apprehension and detention of undocumented persons, with emphasis placed on the rapid growth of biometric capabilities. Case management is where this targeted profiling of individuals comes together.

3.2. Palantir: A New Foundation for ICE Case Management and Analytics

In 2011, DHS signed a contract with defense contractor Raytheon to update its case management system, known as TECS, which had been around since 1987—predating DHS—and was used by both ICE and CBP. For ICE, the system was the "primary investigative tool used to document and build cases for prosecution," while CBP used the system to determine admissibility of nearly 1 million individuals at the border on a daily basis and for information sharing with other federal law enforcement agencies. However, the development of the new system soon ran into technical difficulties, and by February 2014 representatives of the two agencies found themselves testifying before the House Committee on Homeland Security to explain how ICE had wasted some USD 60 million on its part of the project with no deliverables to show for their efforts.[49]

At that hearing, ICE's CIO explained that his agency was already looking into commercial off-the-shelf (COTS) options to start the whole process over with a new contractor to have a replacement system up and running as soon as possible. The new system would ultimately be a hybrid COTS/custom solution developed by Palantir USG, which signed a USD 53.1 million contract in September 2014 for the ICE TECS Modernization program.[50] The CBP TECS platform was taken on by Northrop Grumman, which signed a contract in September 2014 worth up to USD 407 million through the end of 2018.[51]

[49] Hearing before the Subcommittee on Oversight and Management Efficiency of the House Committee on Homeland Security, "Examining challenges and wasted taxpayer dollars in modernizing border security IT systems," February 6, 2014, transcript published by U.S. Government Publishing Office, https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg88024/html/CHRG-113hhrg88024.htm.
[50] Award ID HSCETC14C00002, https://www.usaspending.gov/#/award/23844178.
[51] HSBP1014C00049. See Business Case for CBP TECS Modernization at U.S. Government IT Dashboard, https://itdashboard.gov/drupal/reports/business-case-pdfs.

Palantir's solution for ICE came to be known as the Integrated Case Management (ICM) system, now the "core law enforcement case management tool" used by HSI. ERO also uses the system to manage immigration cases presented for criminal prosecution and queries the system for information that supports its civil immigration enforcement cases.[52]

This was not Palantir's first ICE contract, and in fact the company had received seed funding from In-Q-Tel, a company that invests in tech companies on behalf of the CIA, in its early years.[53] Palantir began providing software to HSI in 2011,[54] and signed a contract for operations and maintenance support services for its Palantir Government software (now Palantir Gotham) in 2013,[55] which it renewed in 2015 on a USD 39.3 million contract, after having already received over USD 19 million from DHS.[56] These contracts were dedicated to the development of the FALCON Search and Analysis (FALCON-SA) application used by ICE as an analytical tool to "store, search, analyze and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil and administrative laws."[57]

Palantir's ICM and FALCON-SA systems work in tandem. ICM is a repository for personally identifiable information from other ICE and CBP systems, commercial data sources and the FBI's National Crime Information Center (NCIC), which interfaces with federal, state and local law enforcement. Meanwhile, FALCON-SA is an analytical tool that helps agents analyze all ingested data, identify connections and produce intelligence reports and visuals.

As seen in Figure 7, ICM interfaces with ERO's primary civil case management system, the Enforcement Integrated Database (EID), which contains biometric and personally identifiable information collected by ERO officers. Figure 7 is intended to highlight the key case management systems within ICE, and for simplicity's sake does not include all systems or interfaces. Further interoperability with law enforcement and foreign governments, particularly regarding biometric information, is detailed visually elsewhere in the report.

All components of ICM are currently being migrated to Amazon Web Services (AWS) GovCloud through a third party. In other words, HSI's "core law enforcement case management tool," with interface connectivity to numerous other data systems at every level of government—and even internationally—will be housed on the Amazon cloud. This is not an isolated case but part of a mass migration of DHS applications onto commercial cloud service providers, particularly Amazon cloud services.

---

[52] DHS, Privacy Impact Assessment for ICE Investigative Case Management, June 16, 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.

[53] SharesPost Palantir company report, sharespost.com/downloads/SharesPost_Palantir_Company_Report.pdf. For information on In-Q-Tel, see: Rick E. Yannuzzi, "In-Q-Tel: A New Partnership Between the CIA and the Private Sector," www.cia.gov/library/publications/intelligence-history/in-q-tel.

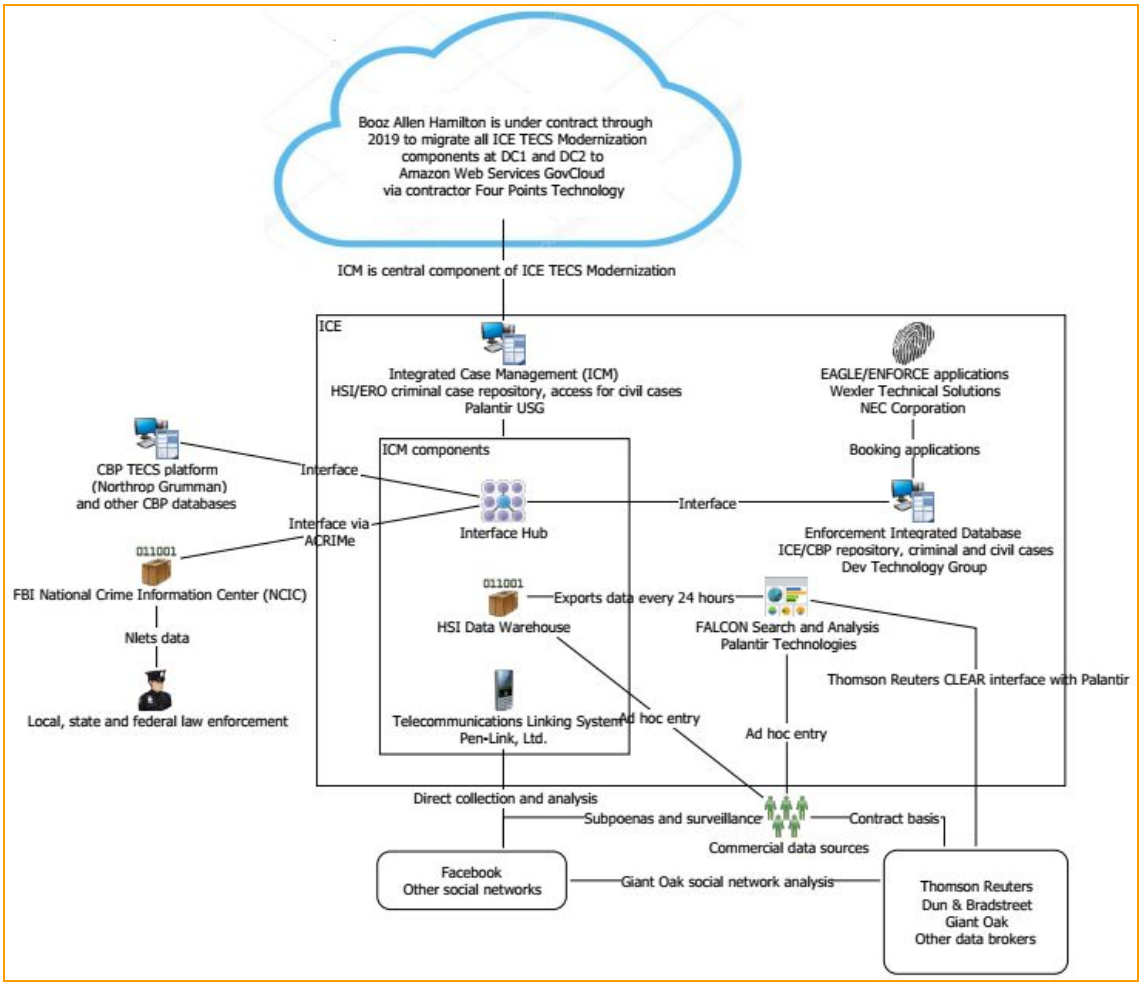
[54] Award ID HSCETE11F00125, https://www.usaspending.gov/#/award/23846894.

[55] Award ID HSCETC13F00030, https://www.usaspending.gov/#/award/23843927.

[56] See ICE contracts awarded to Palantir at: https://www.usaspending.gov/#/search/05cbd3b131948a0852224bb0c5fa017a.

[57] DHS, Privacy Impact Assessment Update for FALCON Search & Analysis System, October 11, 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-032-falcons-b-october2016.pdf.

Figure 7. ICE case management systems and key contractors



Source: Empower LLC image, based on DHS Privacy Impact Assessments for ICM, EID and FALCON-SA; ICE contracts.

Other contractors working on the ICE TECS Modernization program to implement Palantir's ICM system include IntegrityOne Partners[58] and Booz Allen Hamilton,[59] which are providing services including migration to AWS GovCloud, where third-party provider Four Points Technology will host the new Palantir system. CSRA, bought in April 2018 by General Dynamics, will also aid the project as the primary

[58] DHS, ICE Office of Acquisition Management, Limited Source Justification for Award ID HSCETC13F00035, May 15, 2018, https://govtribe.com/project/tecs-mod-leiss-and-data-migration.

[59] DHS, ICE Office of Acquisition Management, Limited Source Justification for Award ID HSCETC14F00041, May 15, 2018, https://govtribe.com/project/tecs-mod-tech-assistance.

contractor at Data Center 1 in Stennis, Mississippi, which still houses some components of the project. Table 6 includes all contractors working on the project; total award amounts are not necessarily exclusive to work on the ICM project.

Table 6. Contractors for ICE TECS Modernization (Integrated Case Management)

Contractor	Total Amount (USD)	Award ID	Description from Business Case document[60]
Prizum Inc. (IntegrityOne Partners, Inc.)	14,013,079	HSCETC13F00035	The Contractor shall provide data migration and synchronization support to the ICE TECS Mod Program for the ICM system. The contractor shall define and develop components that are needed to successfully migrate data from the legacy CBP TECS system to the ICE ICM System and synchronize data between those systems during production operation.
Booz Allen Hamilton	21,528,265	HSCETC14F00041	The scope of work is to provide technical assistance to the ICE TECS Modernization Program during the development and implementation of the ICM solution. Work to be performed includes: systems engineering support for the overall ICE TECS Mod Program, design, develop, test, and deploy the ICE Data Warehouse, support disaster recovery planning and implementation, and System Portfolio analysis.
Palantir USG, Inc.	53,148,388	HSCETC14C00002	The Contractor shall implement, integrate, and test the ICM system and provide O&M support after Initial Operational Capability and Full Operational Capability. The Contractor shall provide and support a phased implementation and enhancement of the ICE ICM which supports the objectives to include: create and manage ICE/HSI investigative cases, links subject records to reports of investigation and cases, shares data with CBP, and performs investigative research internal and external to ICE/DHS.
Deloitte Consulting	9,824,069 10,445,857	HSCETC15F00019 HSCEMS15J00062	The Contractor shall follow Training and Communications best practices to assist the Government in Training services to include the assessment, design, and delivery of training for the modernized system. Communications services shall include the assessment, design, and delivery of communications related to the ICE TECS Modernization

[60] Accessible via U.S. Government IT Dashboard at https://itdashboard.gov/drupal/reports/business-case-pdfs.

			Program and key stakeholders impacted by the transition to the modernized system.
Global Networks Systems of Maryland	3,099,117	HSCETC15J00013	The Contractor shall follow Test and Evaluation (T&E) best practices to assist the Government. The T&E best practices will adhere to DHS Systems Engineering Life Cycle (SELC) and ICE System Lifecycle Management (SLM). All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. All developed solutions and requirements shall be compliant with the HLS EA.
CSRA (General Dynamics)	71,782,797	HSHQDC16D00001	The scope of work will also include all O&M services provided by the DC1 Contractor for future ICE IT Infrastructure or Applications not currently hosted within DC1 that will require migration support services, on-site installation stand-up & configuration services, project management support services, ad hoc services as necessary, followed by ongoing O&M support services once the new migration has been successfully completed.
Four Points Technology	22,727,919	HSCETE16J00343	Provides AWS GovCloud Hosting for the ICE TECS MOD Program.

Source: U.S. Government IT Dashboard, Business Case for ICE TECS Modernization.

When IntegrityOne Partners signed the above contract to work on the ICE TECS Modernization, assisting with services including migration to the Amazon cloud, the company's Federal Strategist was Bill McElhaney, who had worked as Director of Systems Development at ICE from 2006 to 2011. In 2015, McElhaney was promoted to Partner at IntegrityOne.[61] In March 2018, McElhaney walked back through the revolving door when he was appointed CIO at USCIS, where he replaced Mark Schwartz, who had left the agency to work as Enterprise Strategist at Amazon Web Services[62] after having spearheaded a near complete migration of USCIS systems to the Amazon cloud.[63] The revolving door between federal government and IT contractors, particularly cloud service providers, is a wide-spread phenomenon at the highest levels of government.

[61] "McElhaney Promoted to Partner," PR Newswire, June 30, 2015, https://www.prnewswire.com/news-releases/mcelhaney-promoted-to-partner-300106643.html.
[62] Jason Miller, "Former DHS executive to return to be USCIS CIO," Federal News Radio, February 23, 2018, https://federalnewsradio.com/cio-news/2018/02/former-dhs-executive-to-return-to-be-uscis-cio/.
[63] Derek Major, "How USCIS went agile and open to move application process online," GCN, October 29, 2015, https://gcn.com/articles/2015/10/29/uscis-agile-forms.aspx?m=1; Steven Nelson, "Amazon spotlights work with federal immigration agency," Washington Examiner, June 21, 2018, https://www.washingtonexaminer.com/news/white-house/amazon-spotlights-work-with-federal-immigration-agency.

3.3. Biometric Data Storage and Sharing: Interoperability on the Cloud

The CBP component of the TECS Modernization—developed by Northrop Grumman as Palantir took over the ICE component—focused on improving the effectiveness and efficiency of inspection processes at border ports of entry, and improving technological and data sharing functions at land, air and sea ports of entry, particularly for person-centric information.[64] CBP also uses the Enforcement Integrated Database (EID), which is managed by ICE, for case management of enforcement operations in their area of jurisdiction—cases that are not necessarily related to border crossings. These systems, along with the many other data systems at DHS, collect all kinds of personally identifiable information, but they increasingly collect and share biometric information as well.

DHS agencies store all biometric data in the department's Automated Biometric Identification System (IDENT), which backs up data on the AWS cloud.[65] IDENT contains nearly 230 million unique identities, mostly fingerprint records, as well as 36.5 million face records and 2.8 million irises, with the ability to house palm prints, scars and tattoos.[66] DHS is currently developing a new, cloud-based biometric system to replace IDENT, which will have greater storage and matching capabilities, particularly for face and iris, and improved overall performance, as well as planned options for voice, DNA and other biometric modalities. Companies providing cloud services to the new Homeland Advanced Recognition Technology (HART) system, as it is known, remain undisclosed. Northrop Grumman is developing HART after winning a contract worth more than USD 94 million through 2021; the system is scheduled to be operational by late 2019.

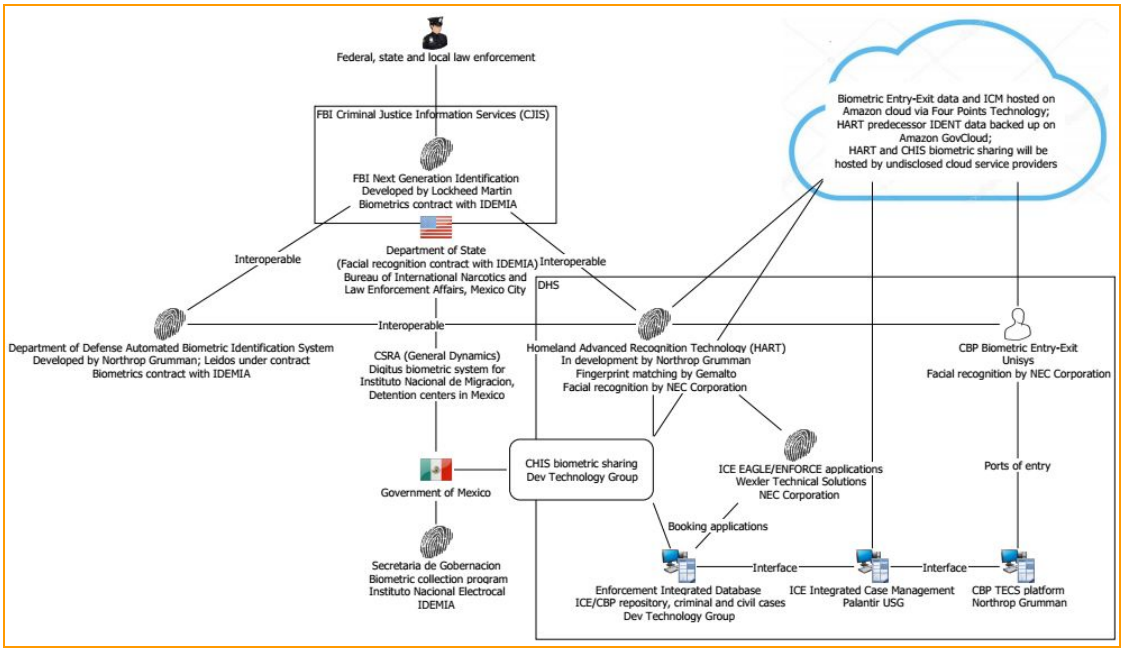
HART and IDENT are interoperable with biometric databases controlled by other U.S. government and international partners, as diagrammed—in simplified fashion—in Figure 8. These databases draw on biometric information collected at two points, broadly speaking: border crossings, overseen by CBP, and other apprehension and detention operations, overseen by ICE but with the participation of CBP in its area of jurisdiction within 100 miles of the border.

Figure 8. DHS biometric data systems and sharing

[64] CBP TECS Modernization Business Case, U.S. Government IT Dashboard, https://itdashboard.gov/drupal/reports/business-case-pdfs.

[65] See Award ID HSHQDC16J00145 for reference to IDENT data back-up, https://www.usaspending.gov/#/award/24243314.

[66] Calvin Biesecker, "Northrop Grumman Begins Development Of Next-Generation DHS Biometric System," May 7, 2018, Defense Daily, www.defensedaily.com/northrop-grumman-begins-development-next-generation-dhs-biometric-system/?fullview=1.



Source: Empower LLC image, based on DHS Privacy Impact Assessments for ICM, EID, CBP TECS and CBP Biometric Entry-Exit; DHS contracts and Mexican government records.

Biometric collection systems at border crossings, including airports, are currently in rapid development. President Trump's 2018 Executive Order 13780, "Protecting the Nation from Foreign Terrorist Entry into the United States,"[67] directed CBP to expedite its Biometric Entry-Exit project, which had been in trial stages since 2016. In response, CBP awarded major contracts—including one to the primary contractor, Pennsylvania-based Unisys, of nearly USD 230 million through the EAGLE II contracting vehicle—to implement systems that would allow for supplementing documents such as passports with biometric information for travelers entering and exiting the United States.[68] The program's emphasis is on exiting travelers, where very little biometric oversight exists. The 2016 contract, deemed Integrated Traveler Initiatives, is the newest iteration of the company's 2010 CBP contract for the Land Border Integration project. The project has deployed facial recognition technology at 10 airports,[69] aiming to identify "individuals who may be subject to law enforcement action." If facial recognition does not confirm a match, a mobile fingerprint device is used to check the departing traveler in IDENT, the DHS biometric database. If no match is found, a check is run through the FBI's biometric database, Next Generation Identification (NGI), and the biometric information is shared with the DHS Office of Biometric Management, which houses IDENT and HART.

[67] Executive Order 13780, March 6, 2017, https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states-2/.

[68] Award ID 70B04C18F00000039, https://www.usaspending.gov/#/award/8287727. See also: CBP Biometric Entry-Exit Business Case, https://itdashboard.gov/drupal/reports/business-case-pdfs.

[69] As of February 2018, "CBP is currently demonstrating facial recognition exit technology at eight U.S. airports, Hartsfield-Jackson Atlanta International Airport, Washington Dulles International Airport, George Bush Intercontinental Airport, Chicago O'Hare International Airport, McCarran International Airport, Houston William P. Hobby Airport, John F. Kennedy International Airport and Miami International Airport. CBP is also collaborating with airline partners to integrate facial recognition technology as part of the boarding process at Hartsfield-Jackson International Airport, John F. Kennedy International Airport and Boston Logan International Airport." See: CBP, "CBP Meets with Privacy Groups to Discuss Biometric Exit," February 2, 2018, https://www.cbp.gov/newsroom/national-media-release/cbp-meets-privacy-groups-discuss-biometric-exit-0.

The Biometric Entry-Exit program is currently limited to CBP but future iterations may involve ICE and the Transportation Security Administration (TSA). CBP has disclosed that airlines, ocean cruise lines and port authorities participate in the program, and partnerships are in place with Delta and JetBlue, which may deploy their own technology to submit photographs for facial recognition.[70] Like Palantir's Integrated Case Management system at ICE, CBP's Biometric Entry-Exit system will be hosted at least partially by Amazon Web Services via third-party Four Points Technology.[71] Data from the IDENT database itself is also backed up on Amazon cloud services.[72]

In addition to border-crossing biometric collection, ICE and CBP collect biometric information during enforcement operations with mobile devices and upload this information to the Enforcement Integrated Database. Equipment used by ICE agents in the field includes the NEC NeoScan fingerprint device[73] and a mobile app called EDDIE developed by Wexler Technical Solutions.[74] EID, in addition to its interface with Palantir's new ICM case management system—the other major case management system at ICE—is linked to the HART/IDENT database. Furthermore, it is the database used for biometric sharing with the Mexican government via the Criminal History Information Sharing (CHIS) program.

3.4. Biometric Sharing with the Mexican Government

To supplement airport biometric collection, CBP signed the Implementing Arrangement Regarding the Sharing of Border Crossing Data with Mexico's National Migration Institute (INM) in August 2017 to exchange biographic information about pedestrians leaving the United States. The project's first phase involves information only about Mexican nationals, though the program will be expanded to share biographic information about all pedestrian travelers with a long-term goal of implementing a "comprehensive biometric exit land solution."[75] CBP tested biometric land exit commercial products (facial and iris scanning) in 2015 and 2016 at the Otay Mesa, California border crossing.[76] The DHS summary report for this testing found that "no technology performed operational matching at a satisfactory level" in the field.[77]

---

[70] CBP, "Biometric Air Exit," https://www.cbp.gov/travel/biometrics/air-exit. See also: CBP Biometric Entry-Exit Business Case, U.S. Government IT Dashboard, https://itdashboard.gov/drupal/reports/business-case-pdfs, and Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-appendixb-july2018.pdf.

[71] Award ID HSBP1017J00789, https://www.usaspending.gov/#/award/23783978. See also: CBP Biometric Entry-Exit Business Case, U.S. Government IT Dashboard, https://itdashboard.gov/drupal/reports/business-case-pdfs.

[72] See Award ID HSHQDC16J00145 for reference to IDENT data back-up, https://www.usaspending.gov/#/award/24243314.

[73] Award ID HSCETE17J00357, https://www.usaspending.gov/#/award/23851115.

[74] Bianca Spinosa, "EDDIE, ICE and apps," FCW, May 28, 2015, https://fcw.com/articles/2015/05/28/eddie-ice-and-apps.aspx.

[75] CBP, "US, Mexico Announce Pilot to Enhance Border Security at San Ysidro-El Chapparral Port of Entry," https://www.cbp.gov/newsroom/national-media-release/us-mexico-announce-pilot-enhance-border-security-san-ysidro-el. See Privacy Impact Assessment for United States-Mexico Entry/Exit Data Sharing Initiative, December 14, 2017, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-usmexicoentryexitdatasharinginitiative-december2017.pdf

[76] Privacy Impact Assessment Update for the Southwest Border Pedestrian Exit Field Test, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp027-swbpedestrianexit-march2018.pdf

[77] DHS, Southern Border Pedestrian Field Test, Summary Report, https://epic.org/foia/dhs/cbp/biometric-entry-exit/Southern-Border-Pedestrian-Field-Test-Report.pdf.

Biometric kiosks were installed in three major Mexican airports (Mexico City, Los Cabos and Cancun) in 2018 by Swiss company SITA.[78] While there is no evidence of an information sharing agreement in place, and the program is aimed at tourist destinations for the time being, Mexico's National Migration Institute already shares border crossing data with CBP and has a biometric sharing agreement in place with the U.S. Department of State, to be addressed below.

Biometric data collected by all DHS agencies, including USCIS, CBP and ICE, is fed into IDENT. IDENT is, and HART will be, interoperable with the FBI's NGI biometric database and the Department of Defense's Automated Biometric Identification System, meaning that biometric information submitted to any of those agencies can be accessed by the others. The FBI's data sharing with local and state law enforcement means that DHS has access to virtually any biometric data from domestic law enforcement it wishes to access.

DHS also shares biometric data with the government of Mexico through the CHIS program. This sharing is facilitated through the EID case management system, and as of 2016 allows for the sharing of biometric information from the U.S. government with Mexico regarding individuals deported from the United States and who were convicted of certain felonies in the United States.[79] CHIS also allows for the sharing of convictions in partner countries with DHS. As of 2016, DHS had CHIS agreements with Mexico, El Salvador, Guatemala, Honduras, Mexico, the Dominican Republic, Jamaica and the Bahamas.[80]

This process had been entirely manual until recently, but contractor Dev Technology, which has already done operations and maintenance work on EID,[81] recently developed a secure web service to facilitate biometric sharing between EID and the Mexican government through contracts with both CBP and the Department of State.[82] Dev Technology has also won multiple ICE contracts and is the biggest recipient of EAGLE II funding for ICE.

The U.S. government collaborates with Mexico on biometric collection beyond the scope of CHIS. Working through the Department of State, specifically its Bureau of International Narcotics and Law Enforcement Affairs (INCLE) in Mexico City, the U.S. government commissioned the building of a biometric system for Mexico's National Migration Institute (INM) in 2017.[83] CSRA, now owned by General Dynamics, was contracted for the job, which is known as the Digitus Agreement and was given a budget of approximately USD 75 million under the Merida Initiative. According to reporting in Mexico,[84] the Digitus contract is

[78] Karla Rodríguez, "La firma de los kioscos migratorios va por nuevos aeropuertos," *El Financiero*, April 4, 2018, www.elfinanciero.com.mx/empresas/la-firma-de-los-kioscos-migratorios-va-por-nuevos-aeropuertos.
[79] DHS Privacy Impact Assessment Update for the Enforcement Integrated Database (EID) Criminal History Information Sharing (CHIS) Program, January 15, 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-eidchis-january2016.pdf.
[80] DHS Congressional Budget Justification FY 2017, Volume II, https://preview.dhs.gov/sites/default/files/publications/FY%202017%20Congressional%20Budget%20Justification%20-%20Volume%202_1.pdf.
[81] Award ID HSCETC12F00005, https://www.usaspending.gov/#/award/23843861.
[82] Dev Technology Group, "Services We Provide," devtechnology.com/new/wp-content/uploads/2018/06/Dev-Technology-Capabilties-2018-02.pdf. See also: Award ID 19MX9018C0002, https://www.usaspending.gov/#/award/5845750; and Award ID 70B04C18F00000490, https://www.usaspending.gov/#/award/67072955.
[83] Award ID SAQMMA17F2623, https://www.usaspending.gov/#/award/27916327.
[84] J. Jesús Esquivel, "Washington usa al gobierno mexicano para afirmar sistemas de espionaje antimigratio," Proceso 2166, May 6, 2018, accessible at: https://prensaindigena.org/web/pdf/Proceso-2166.pdf.

intended to support biometric collection of Central Americans being held at detention centers in Mexico—information that is corroborated by a DHS Privacy Impact Assessment, which reveals:

> The Government of Mexico will submit its collected biometric and biographic holdings, in bulk, to DHS [...] on individuals whom they believe to be nationals of a third country. [...] Mexico will determine whether an individual is believed to be a national of a third country based on data such as application responses, identity documentation, or the nature of the application or investigation, and who have been interdicted, and detained at National Institute of Migration (INM) Migration Stations nationwide.[85]

The Digitus program is enabled by a series of bilateral agreements between DHS and the Mexican government:[86]

- On April 29, 2011, an Interconnection Security Agreement (ISA) was signed between Jose Francisco Blake Mora of the Secretariat of Governance for the United Mexican States (SEGOB) and DHS Secretary Janet Napolitano. This ISA created a partnership between the government of Mexico and DHS to "efficiently, securely, and uniformly facilitate and regulate the flow of information among relevant agencies, areas, and components."[87]
- On April 17, 2013, a Memorandum of Cooperation and action plan between DHS and SEGOB was signed by Secretary Napolitano and Secretary of Interior Osorio Chong. The action plan covered six areas:
  1. Effective management of passenger flows and attention to migrants from third countries.
  2. Facilitating the safe repatriation of Mexican nationals.
  3. Combating the criminal activities associated with migratory flows.
  4. Strengthening security conditions in the border region between Mexico and the United States.
  5. Prevention of security threats in both countries.
  6. Collaboration in attending to natural disasters and emergencies.

  In addition to calling for an increase in the collection of biometric data from undocumented third-country nationals detained in Mexico, the action plan called to "jointly examine approaches to extend the detention times of third-country nationals" and for the "exchange of criminal background information related to Mexican nationals to be repatriated" (what would later become the Criminal History Information Sharing agreement).[88]

- In January 2017, a Statement of Cooperation (SOC) between DHS and SEGOB's National Migration Institute (INM) was signed. The SOC governs the exchange of biometric and biographic data between both countries, which seek to exchange identity information on third-country nationals

[85] IDENT Privacy Impact Assessment, Appendix CC, "U.S. Mexico Biometric Immigration Information Sharing," https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-identappendices-november2017.pdf.
[86] Empower LLC obtained copies of the 2013 Memorandum of Cooperation and 2017 Statement of Cooperation from the Mexican government via public records requests.
[87] IDENT Privacy Impact Assessment, Appendix CC, "U.S. Mexico Biometric Immigration Information Sharing," https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-identappendices-november2017.pdf.
[88] Quoted text translated from the Spanish version of the document, obtained by Empower LLC from the Mexican government via public records request: "Memorandum de Cooperación entre la Secretaría de Gobernación de los Estados Unidos Mexicanos y el Departamento de Seguridad Nacional de los Estados Unidos de América."

seeking authorization to travel, work or live in Mexico or the United States, or who have been detained by INM.[89] The personal data exchanged may include:

1. Relevant biometrics, including digital prints, and, when available and appropriate, facial images, irises or other unique physical identifiers.
2. Record of unique transactions, data associated with contacts with the authorities or reference numbers that help to identify an individual.
3. Any associated biographic information, including information provided by the third-country national.
4. Data associated with contacts with the authorities.
5. Transactional metadata, such as date of contact with the authorities and time stamp.[90]

The agreements enable the Mexican government to submit electronic fingerprint queries to the DHS' fingerprint database, and all biometric and associated biographic information obtained by Mexico on migrants will be enrolled in the DHS fingerprint repository.[91]

The Mexican government has handed over dozens of fugitives and "Special Interest Aliens" under the Digitus program, which over a thirteen-month period in 2017 and 2018 collected biometrics from over 30,000 people in INM detention centers in Mexico City and along the southern Mexican border. Biometric collection under the program has reportedly also been performed at non-INM prisons, and is being extended to INM prisons in Tijuana, Mexicali and Reynosa.[92]

The Department of State characterizes this as a drug trafficking initiative in its FY 2019 congressional budget justification: "INCLE programs will expand a biometrics project in Mexico to enable data sharing and improve capabilities to address the heroin and fentanyl crisis and illicit revenue streams funding transnational criminal organizations."[93] However, the CSRA contract for project implementation is far broader in scope—in keeping with the reported blanket application of the program in INM prisons—calling for "enduring biometrically-based identity management services to the Government of Mexico and its mission partners that will enable informed decision-making by producing accurate, timely and high-assurance identity information and analysis in compliance with the Digitus Agreement under the Merida Initiative."[94]

William Brownfield, head of INCLE until his retirement in 2017, frankly admitted to Washington Post reporters that the biometrics program is about controlling immigration from Central America: "Part of the reason the Mexican government was interested is that it brought them value by giving them a window

[89] IDENT Privacy Impact Assessment, Appendix CC, "U.S. Mexico Biometric Immigration Information Sharing," www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-identappendices-november2017.pdf," https.
[90] Quoted text translated from the Spanish version of the document, obtained by Empower LLC from the Mexican government via public records request: "Declaración de Cooperación entre el Departamento de Seguridad Nacional de los Estados Unidos de América y la Secretaría de Gobernación de los Estados Unidos Mexicanos, Instituto Nacional de Migración, Referente al Intercambio de Información Biométrica de Inmigración."
[91] IDENT Privacy Impact Assessment, Appendix CC, "U.S. Mexico Biometric Immigration Information Sharing," https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-identappendices-november2017.pdf.
[92] J. Jesús Esquivel, "Washington usa al gobierno mexicano para afirmar sistemas de espionaje antimigratio," Proceso 2166, May 6, 2018, accessible at: https://prensaindigena.org/web/pdf/Proceso-2166.pdf.
[93] Congressional Budget Justification, Department of State Foreign Operations, and Related Programs, FY 2019, https://www.state.gov/documents/organization/277155.pdf.
[94] Award ID SAQMMA17F2623, https://www.usaspending.gov/#/award/27916327.

into who was coming into Mexico, as well as those simply en route to the United States. And from the U.S. side, we accepted and understood that it is a lot easier, cheaper and more efficient to manage migrant flows from Central America to the U.S. at Mexico's much smaller southern border than at our longer and more complicated [U.S.-Mexico] border." U.S. officials told the reporters that "the goal is to have the capability to screen every migrant taken into custody in Mexico."[95]

[95] Joshua Partlow and Nick Miroff, "U.S. gathers data on migrants deep in Mexico, a sensitive program Trump's rhetoric could put at risk," Washington Post, April 6, 2018, https://www.washingtonpost.com/world/national-security/us-gathers-data-on-migrants-deep-in-mexico-a-sensitive-program-trumps-rhetoric-could-put-at-risk/2018/04/06/31a8605a-38f3-11e8-b57c-9445cc4dfa5e_story.html?utm_term=.287492b18ba0.

4. Information Sharing with Local, State and Federal Law Enforcement

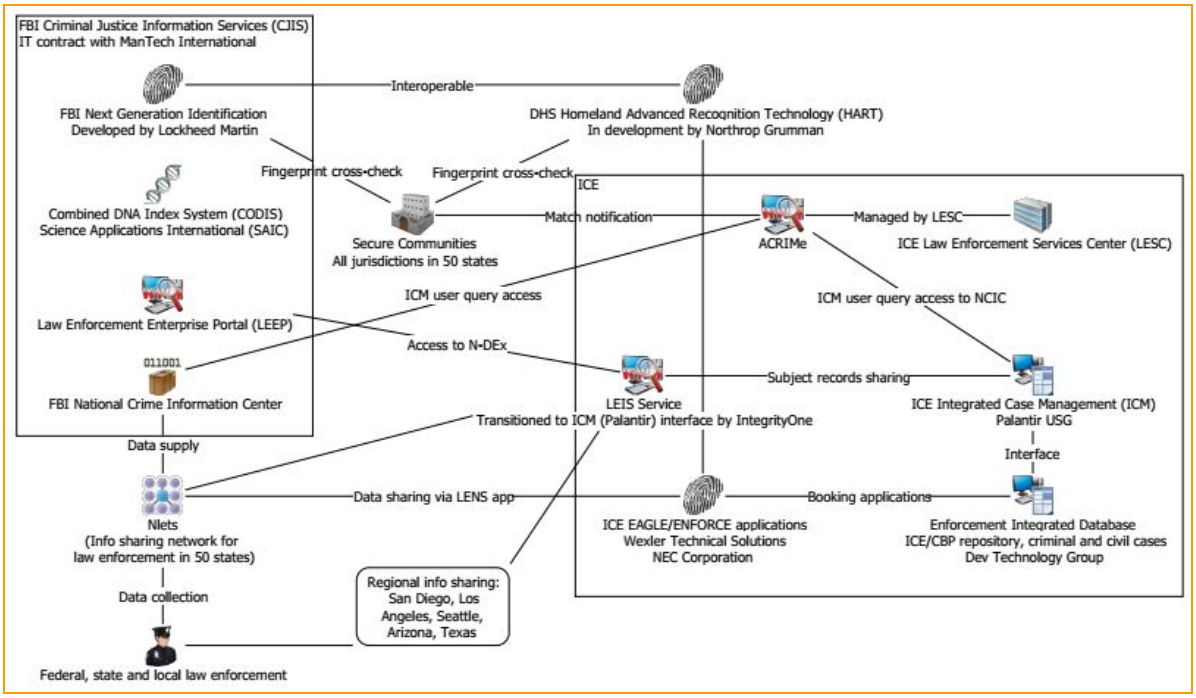
4.1. ICE's Law Enforcement Support Center and FBI Information Sharing

ICE collaborates with local, state and federal law enforcement in numerous ways, but perhaps most directly through two programs:

- 287(g): ICE delegates immigration enforcement authority to state and local agencies through Memoranda of Agreement (currently 78 agencies in 20 states[96]).
- Criminal Alien Program (CAP): Gives ICE agents direct access to jails to target individuals for deportation based on biographic and biometric identification.[97]

There are other forms of collaboration between ICE and local, state and federal law enforcement based on information sharing, most notoriously through the Secure Communities program, which cross-checks fingerprints of incarcerated individuals between the DHS biometric database and the FBI biometric database. However, ICE agents have a whole array of information sharing agreements and data systems in place, outside the confines of jails and prisons (see Figure 9).

Figure 9. ICE information sharing with local, state and federal law enforcement



Source: Empower LLC image, based on DHS Privacy Impact Assessments for ICM, EID and ACRIMe; ICE contracts; ICE and CJIS websites

[96] ICE, Delegation of Immigration Authority Section 287(g) Immigration and Nationality Act, https://www.ice.gov/287g.
[97] ICE, Criminal Alien Program, https://www.ice.gov/criminal-alien-program.

Principal among ICE agents' tools for wide-reaching access to personally identifiable information from local, state and federal law enforcement information is their access to the FBI's National Crime Information Center (NCIC), which contains information on both "criminal targets" and "immigration violators," including civil cases.[98] NCIC contains information from Nlets, a state-owned network of law enforcement agencies.[99] Nlets "links together and supports every state, local and federal law enforcement, justice and public safety agency for the purposes of sharing and exchanging critical information,"[100] processing some 1.5 billion transactions each year.[101] The network also shares information with Interpol and Canadian authorities. Nlets includes a vast amount of information including diverse biographic data, criminal histories, motor vehicle data and driving history, driver's license photos from some states,[102] and even license plate reader data collected by CBP.[103]

NCIC is one part of the FBI's Criminal Justice Information Services (CJIS) complex, based in Clarksburg, West Virginia. In 2017, the FBI awarded ManTech International, headquartered in Northern Virginia, a contract worth USD 220 million for IT services at CJIS.[104] (The following day, ManTech International was awarded a USD 229 million contract by CBP under the DHS EAGLE II contracting vehicle.)[105] CJIS also houses the following FBI systems, among others:

- The Next Generation Identification (NGI) biometric database, interoperable with DHS's new HART biometric database, which together support the Secure Communities program by cross-checking fingerprints.
- The Combined DNA Index System (CODIS).
- The Law Enforcement Enterprise Portal (LEEP), which houses the National Data Exchange System (N-DEx), an "unclassified national information-sharing system that enables criminal justice agencies to search, link, analyze, and share local, state, tribal, and federal records" across jurisdictions. N-DEx provides access to commercial programs such as Forensic Logic's COPLINK.[106]

Palantir's new Integrated Case Management (ICM) system for ICE plays a key role in this information sharing with law enforcement. ICE agents access NCIC data from within ICM via ICE's Alien Criminal

[98] DHS, Privacy Impact Assessment for ICE Investigative Case Management, June 16, 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.
[99] DHS, Privacy Impact Assessment Update for the Enforcement Integrated Database (EID) Law Enforcement Notification System (LENS), September 22, 2015, https://www.dhs.gov/sites/default/files/publications/PIA%2C%20ICE-EID%20Update%20%28LENS%29%2C%2020150922%2C%20PRIV%20FINAL%20%5Bsigned%5D.pdf.
[100] See archived Nlets webpage at: https://web.archive.org/web/20171007182007/www.nlets.org:80/about/what-we-do.
[101] Archived Nlets document accessible through Wayback Machine at: https://web.archive.org/web/20170701100901/nlets.org/nlets-resources/library?a=downloadRaw&documentid=5380ab4c-4d9b-11e4-ab3f-00155d003202.
[102] National Immigration Law Center, "Glossary at a Glance: Immigration Databases, Information Sharing Systems, and Case Management Systems," January 2018, https://www.nilc.org/wp-content/uploads/2018/01/databases-glossary.pdf.
[103] Cached Nlets informational document. See also: DHS, Privacy Impact Assessment for CBP License Plate Reader Technology, December 11, 2017, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp049-cbplprtechnology-december2017.pdf.
[104] ManTech International, "FBI Awards ManTech $220 Million Contract to Protect Mission-Critical Information Systems for Law Enforcement Community," press release, April 25, 2017, investor.mantech.com/news-releases/news-release-details/fbi-awards-mantech-220-million-contract-protect-mission-critical.
[105] ManTech International, "ManTech Wins $229 Million U.S. Homeland Security Contract for Border Protection," press release, April 26, 2017, investor.mantech.com/news-releases/news-release-details/mantech-wins-229-million-us-homeland-security-contract-border.
[106] FBI, National Data Exchange (N-DEx) System, https://www.fbi.gov/services/cjis/ndex.

Response Information System (ACRIMe).[107] ACRIMe is managed by ERO's Law Enforcement Services Center in Williston, Vermont.

Palantir's ICM system, in turn, shares information with Nlets, with the FBI and through regional law enforcement information sharing agreements via ICE's Law Enforcement Information Sharing (LEIS) Service, which provides filtered information to law enforcement agencies. ICE also shares criminal information on individuals from ERO's Enforcement Integrated Database (EID) with diverse law enforcement agencies, including DHS fusion centers and state and local police, through its Law Enforcement Notification System (LENS), a messaging application.[108] LENS shares biographic information on individuals released from ICE custody with Nlets.

Palantir's ICM system, in conjunction with its FALCON-SA analytical application, appears to be replacing the functions of the ICEPIC tool that gave other law enforcement access to filtered ICE data sources through the LEIS Service interface and helped identify non-obvious relationships among individuals and organizations "that are indicative of violations of the customs and immigration laws." The ICM Privacy Impact Assessment notes that ICEPIC "formerly housed the [LEIS] Service" and will be retired.[109] ICM-related contract documents suggest that LEIS now directly interfaces with Palantir's ICM,[110] though a PIA on ICEPIC scheduled for late 2016 was never released and its role remains unclear.

4.2. DHS Regional Information Sharing Agreements

The Unit Chief at HSI's Law Enforcement Information Sharing Initiative (LEISI)— overseeing the LEIS Service that interfaces with Palantir's ICM—is named Jason Henry.[111] Henry is also ICE's representative at Nlets, the Arizona-based information sharing network for law enforcement across the country and internationally that provides information to the FBI's NCIC database.[112] He was also a member of the Criminal History Information Sharing Working Group (CHIS is the program that guides ICE biometric sharing with Mexico and other countries.)[113]

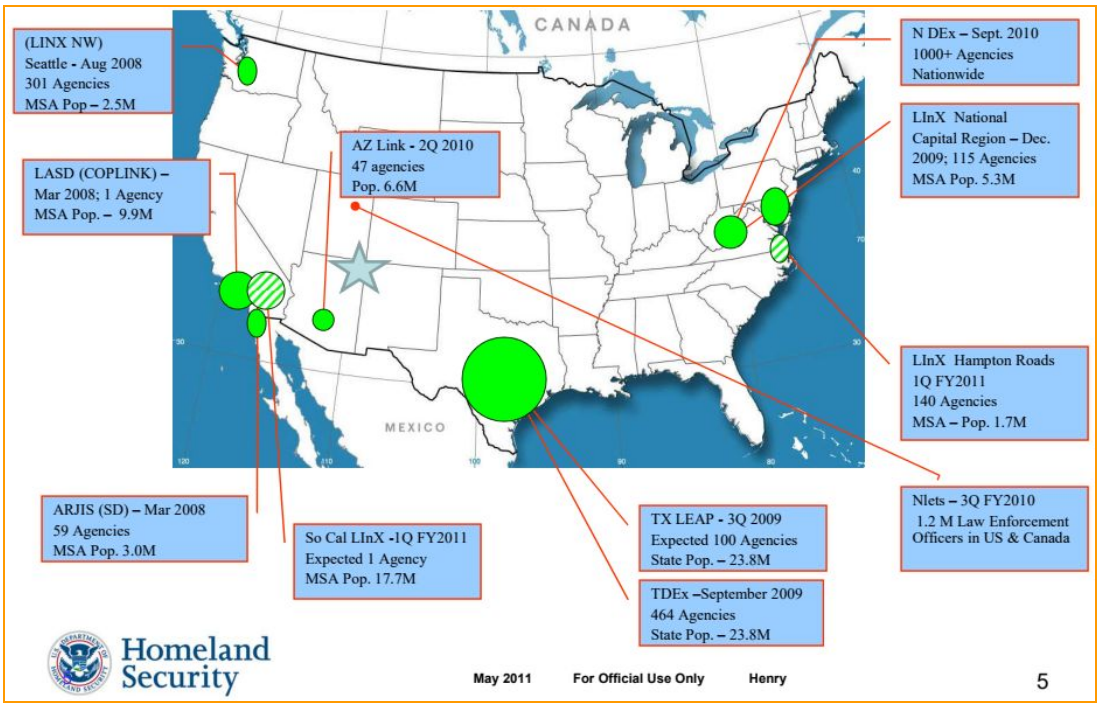
While ICE has not published many details about LEISI, it is clearly a focal point for the agency's efforts to enable information sharing with domestic and international law enforcement. The jurisdictions that participate directly in the program are the laboratory for ICE/police collaboration and subject profiling. This section will take a look at some of those jurisdictions, many of which are located in Southwestern border

[107] DHS, Privacy Impact Assessment for ICE Investigative Case Management, June 16, 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.
[108] LENS is part of the EARM application in EID. See: DHS, Privacy Impact Assessment Update for the Enforcement Integrated Database (EID) Law Enforcement Notification System (LENS), September 22, 2015, https://www.dhs.gov/sites/default/files/publications/PIA%2C%20ICE-EID%20Update%20%28LENS%29%2C%2020150922%2C%20PRIV%20FINAL%20%5Bsigned%5D.pdf.
[109] DHS, Privacy Compliance Review of the ICE Pattern Analysis and Information Collection Law Enforcement Information Sharing Service, December 15, 2011, https://www.dhs.gov/sites/default/files/publications/privacy_privcomrev_ice-analysis.pdf.
[110] DHS, ICE Office of Acquisition Management, Limited Source Justification for Award ID HSCETC13F00035, May 15, 2018, https://govtribe.com/project/tecs-mod-leiss-and-data-migration.
[111] Jason Henry LinkedIn profile, https://www.linkedin.com/in/jason-henry-b5010836/.
[112] Nlets members, archived by Wayback Machine, accessible at: https://web.archive.org/web/20170315231216/www.nlets.org:80/our-members/members.
[113] DHS, The Secretary's Award for Excellence 2014, https://www.dhs.gov/2014-awards-excellence.

states, and at the contractors that work with them, with the aim of identifying key IT and equipment contractors in the collection of biometric and personally identifiable information for DHS collaboration.

In 2011, near the beginning of his tenure at LEISI, Jason Henry presented a map that identified the regional participants in LEISI. These regional participants include all jurisdictions that ICE characterizes as having successfully implemented the LEIS Service as of January 2018: San Diego, Los Angeles, Seattle, Arizona and Texas, as well as the Department of Justice's OneDOJ program[114] (which has now been absorbed by the FBI's N-DEx,[115] originally developed by Raytheon[116]). In May 2017, ICE spokesperson Matthew Bourke claimed that ICE had not established any new agreements since October 2011[117] when a Privacy Impact Statement on ICEPIC was released.[118]

Figure 10. LEIS Service participants as of May 2011



Source: DHS Law Enforcement Information Sharing Initiative, Presentation to Tribal Assistance Coordination Group, May 2011.

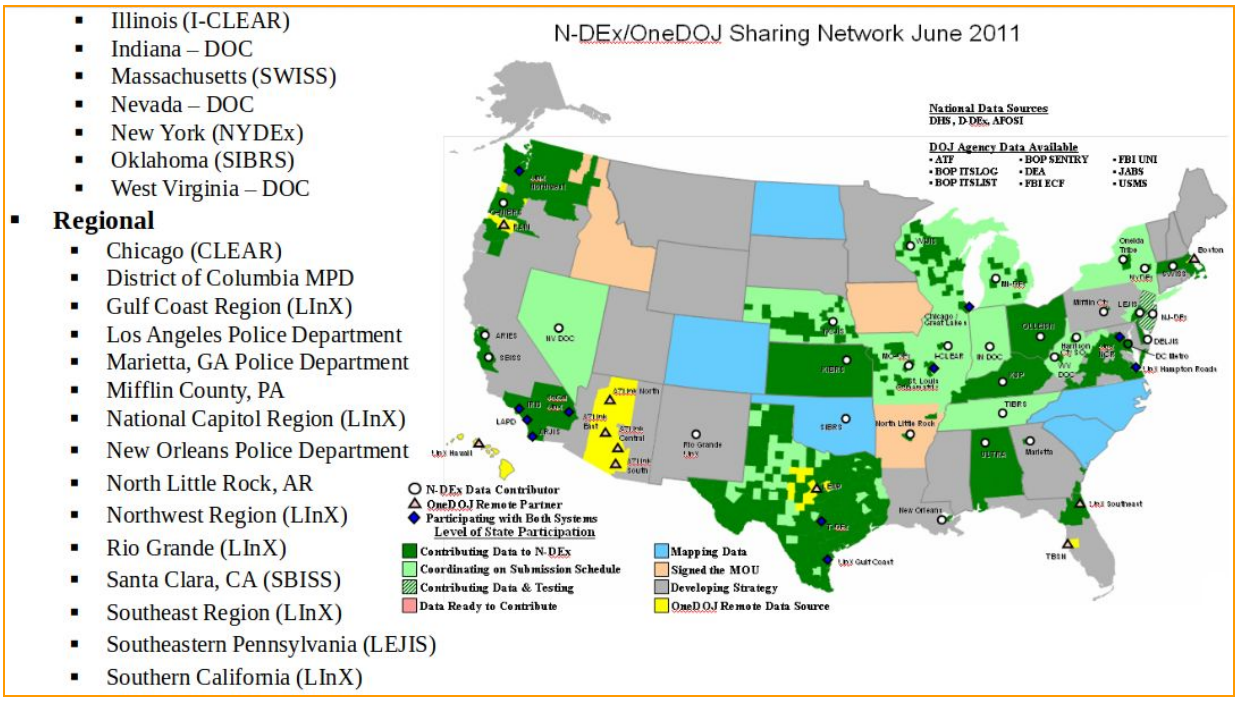
The LInX system, with several regional components using the LEIS Service, was developed by defense contractor Northrop Grumman for the Naval Criminal Investigative Service (NCIS).[119]

---

[114] ICE, Law Enforcement Information Sharing Initiative, https://www.ice.gov/le-information-sharing.
[115] DOJ, Privacy Impact Assessment for the National Data Exchange (N-DEx) System, May 9, 2014, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/N-DEx.
[116] DOJ Award ID DJFA8D802335, https://www.usaspending.gov/#/award/13126669.
[117] George Joseph, "Where ICE Already Has Direct Lines To Law-Enforcement Databases With Immigrant Data," NPR, May 12, 2017, https://www.npr.org/sections/codeswitch/2017/05/12/479070535/where-ice-already-has-direct-lines-to-law-enforcement-databases-with-immigrant-d .
[118] DHS, Privacy Compliance Review of the ICE Pattern Analysis and Information Collection Law Enforcement Information Sharing Service, December 15, 2011, https://www.dhs.gov/sites/default/files/publications/privacy_privcomrev_ice-analysis.pdf.
[119] Northrop Grumman, "Helps Investigators Search Across Jurisdictional Boundaries to Solve Crimes" October 12, 2011, https://news.northropgrumman.com/news/releases/northrop-grumman-selected-for-law-enforcement-information-exchange-follow-on-contract.

The DHS regional agreements in Figure 10 are supplemental to Nlets and the nationwide N-DEx system, managed at the FBI's West Virginia facilities FBI, which includes data from a much wider network of law enforcement agencies. The reach of N-DEx information sharing in 2011 is shown in Figure 11. The system contains diverse biographic data points and photographic identification, and is managed by the FBI's CJIS complex, which also manages the CODIS DNA database and the NGI biometric database. N-DEx has since become available to law enforcement in all states and even to some foreign criminal justice agencies.[120] The network shown in Figure 11 has been expanded across the country, but the graphic gives a sense of the first jurisdictional arrangements. As of August 2015, over 5,300 agencies contributed information to N-DEx.[121]

Figure 11. N-DEx information sharing as of June 2011



Source: ICE, Information Sharing Status, February 23, 2011, https://info.publicintelligence.net/ICE-InformationSharing.pdf.

Most of these information sharing systems are supported by commercial applications. The most common platform used is COPLINK, used by over 5,100 law enforcement agencies across the country and hosted on the cloud at Nlets in Arizona.[122] COPLINK contains diverse information on individuals, organizations, and vehicles, among other things, and allows users to filter individual searches by categories such as race, hair color, eye color, complexion, build, ethnicity, and country of origin, as well as employers, associates,

[120] DOJ, Privacy Impact Assessment for the National Data Exchange (N-DEx) System, May 9, 2014, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/N-DEx.
[121] Kasey Wertheim and Kelly Badgett, "FBI National Data Exchange System's On-Line Tool Enhances Dispatching by Law Enforcement Agencies throughout the US," Annals of Emergency Dispatch & Response, August 1, 2015, https://www.aedrjournal.org/fbi-national-data-exchange-systems-on-line-tool-enhances-dispatching-by-law-enforcement-agencies-throughout-the-us/.
[122] Forensic Logic, "Forensic Logic Announces Acquisition of COPLINK Platform from IBM," press release, October 4, 2017, https://forensiclogic.com/forensic-logic-announces-acquisition-of-coplink-platform-from-ibm/.

hangout spots, and gang-related information.[123] The application was developed at the University of Arizona in 1997 with funding from the National Institute of Justice and the National Science Foundation, in collaboration with The Tucson and Phoenix Police Departments, Tucson CBP and the Pima County Sheriff's Department. COPLINK was developed by the University of Arizona's Artificial Intelligence Laboratory for the purposes of:

- Cross-jurisdictional information sharing, analysis, visualization and research for the law enforcement and intelligence community for border and national security.
- Study policy issues within government agencies and develop a framework for successful information sharing and analysis while taking into consideration the privacy and security of data.
- Develop algorithms that automatically detect false identities to assist police and intelligence investigations.
- Focus on cross-border crime scenarios and organized criminal activity networks to provide value to local and national law enforcement.[124]

In other words, the most widely used information sharing platform for state and local law enforcement was developed specifically for collaboration with federal immigration enforcement.

The Tucson Police Department leads the Southern Arizona hub of DHS LEISI partner AZLink (see Figure 10 above), which was coordinated with DHS funding[125] and is based on the COPLINK application.[126] Another of DHS's LEISI regional partners, the San Diego area's ARJIS, was involved in early COPLINK research,[127] and the Los Angeles Sheriff's Department adopted the technology for its information sharing data warehouse.[128]

COPLINK was first commercialized by Hsinchun Chen, a University of Arizona researcher, through the company Knowledge Computing Corporation (KCC). The company was bought by i2 Limited, a UK company, in 2009, which was in turn bought by IBM in 2011. What became IBM's i2 software, the foundation for COPLINK, is similar to Palantir's Gotham application, used for the DHS FALCON-SA application.

In 2017, IBM sold COPLINK to Northern California company Forensic Logic, which already owned the LEAP application used by LEISI regional partners in Texas, New Mexico and Oklahoma.[129] This amounted

[123] George Joseph, "New Documents Reveal How ICE Mines Local Police Databases Across the Country," The Appeal, April 26, 2018, https://theappeal.org/new-documents-reveal-how-ice-mines-local-police-databases-across-the-country-660e2dfddbe3/.
[124] University of Arizona Artificial Intelligence Laboratory, "Data Warehousing - Coplink*/BorderSafe/RISC," https://ai.arizona.edu/research/coplink.
[125] DHS, "Wireless Stakeout: Using Smartphones to Nab Suspects," https://www.dhs.gov/science-and-technology/wireless-stakeout.
[126] William M. Kalaf, "Arizona law enforcement biometrics identification and information sharing technology framework," master's thesis, Naval Postgraduate School, March 2010, https://calhoun.nps.edu/bitstream/handle/10945/5370/10Mar_Kalaf.pdf?sequence=1&isAllowed=y.
[127] University of Arizona Artificial Intelligence Laboratory, "Data Warehousing - Coplink*/BorderSafe/RISC," https://ai.arizona.edu/research/coplink.
[128] DHS, Privacy Compliance Review of the ICE Pattern Analysis and Information Collection Law Enforcement Information Sharing Service, December 15, 2011, https://www.dhs.gov/sites/default/files/publications/privacy_privcomrev_ice-analysis.pdf.
[129] DHS, Privacy Compliance Review of the ICE Pattern Analysis and Information Collection Law Enforcement Information Sharing Service, December 15, 2011, https://www.dhs.gov/sites/default/files/publications/privacy_privcomrev_ice-analysis.pdf. This LEAP application is confirmed to be the Forensic Logic application at: EJustice Solutions, "EJustice Solutions Record Management Systems

to a major consolidation of information sharing systems in the LEISI program and nationally, and brought most law enforcement information sharing in the Southwestern border states under one corporate roof. Also in 2017, Forensic Logic entered into an agreement for integrated access to Thomson Reuter's CLEAR program, which contains a vast database of public and proprietary information.[130] In the same year, the Department of Justice bought Forensic Logic's LEAP Network for the largest 500 cities in the United States on behalf of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).[131] Forensic Logic now controls a very large segment of the market for direct information sharing between DHS and local and state law enforcement.

The LEAP Network is cloud-based, and while the company does not reveal which cloud provider hosts the service, Forensic Logic partners with Amazon Web Services[132] as part of AWS's Justice and Public Safety program, which sells cloud services to state and local law enforcement across the country based on its compliance with the FBI's CJIS standards (CJIS is the West Virginia facility that manages NCIC, N-DEx, NGI, CODIS and other systems accessible to DHS). As of December 2016, AWS had CJIS agreements in place with the States of Utah, Washington, California, Minnesota, Colorado, Oregon, and Louisiana, among others, enabling law enforcement agencies to "run CJIS workloads in the cloud with the assurance that they are compliant with CJIS standards."[133]

DHS's LEISI also uses Amazon cloud services through the Homeland Security Information Network (HSIN),[134] one of the first DHS components to be migrated to AWS.[135] Jason Henry has been an HSIN Advisory Councilmember since 2010, when he began as Unit Chief of LEISI.[136]

Furthermore, AWS is a sustaining member of the IJIS Institute,[137] an industry organization that is partnered with Nlets[138] and represents companies that "provide products and services to local, state, tribal, and federal agencies for justice, public safety and homeland security information exchange and technology initiatives." AWS was the platinum sponsor of the 2016 IJIS Institute National Symposium in Arlington, Virginia, which featured distinguished speaker Kshemendra Paul, currently the Cloud Action

---

Offers Free Integration With the Texas Law Enforcement Analysis Portal (LEAP)," press release, September 14, 2010, www.marketwired.com/press-release/ejustice-solutions-record-management-systems-offers-free-integration-with-texas-law-1318227.htm.

[130] "Thomson Reuters CLEAR, Forensic Logic/Coplink Plan Data Alliance," Police Magazine, October 28, 2017, https://www.policemag.com/channel/technology/news/2017/10/19/thomson-reuters-clear-forensic-logic-coplink-plan-data-alliance.aspx.

[131] Investment Recovery Partners LLC, Investments Under Management, March 1, 2017, www.irpllc.net/IRPLLC%20Summary%20Active%20Investments%20Report.pdf.

[132] AWS, AWS for Justice and Public Safety, https://aws.amazon.com/stateandlocal/justice-and-public-safety/.

[133] AWS, AWS Signs CJIS Agreement with the State of Utah," December 5, 2016, https://aws.amazon.com/blogs/publicsector/aws-signs-cjis-agreement-with-the-state-of-utah/; AWS, "AWS Signs CJIS Agreement with the State of Washington," October 17, 2016, https://aws.amazon.com/blogs/publicsector/aws-signs-cjis-agreement-with-the-state-of-washington/.

[134] Jason Henry, "HSIN: Supporting Secure Collaboration for Interagency Partners," The HSIN Advocate, September 2014, https://content.govdelivery.com/attachments/USDHSIN/2014/09/29/file_attachments/328378/HSIN-Newsletter-September2014.pdf.

[135] See presentation by HSIN Operations Manager Damon Bragg at 2018 AWS Public Sector Summit, "DHS HSIN's Journey to FedRAMP High on AWS GovCloud (US)," https://www.youtube.com/watch?v=I7EKvHscYSA.

[136] Jason Henry LinkedIn profile, https://www.linkedin.com/in/jason-henry-b5010836/.

[137] IJIS Institute, "IJIS Institute Welcomes Amazon Web Services as Sustaining Member," press release, September 29, 2015, https://cdn.ymaws.com/www.ijis.org/resource/collection/D69CFC9E-624F-4843-A24E-0D9EA22D0439/PR_20150929_-_Amazon_Web_Services_Becomes_IJIS_Sustaining_Member_FINAL.pdf.

[138] Nlets, "Nlets and the IJIS Institute Establish Alliance Partnership to Formally Acknowledge Collaboration," press release, October 16, 2017, https://cdn.ymaws.com/www.ijis.org/resource/collection/D69CFC9E-624F-4843-A24E-0D9EA22D0439/Nlets_IJIS_Alliance_Press_Release_Final_20171017.pdf.

Officer for DHS in charge of that agency's cloud migration. At the time, Paul was Program Manager of the Information Sharing Environment at the Office of the Director of National Intelligence.[139]

Other IJIS sustaining members include Microsoft; Arizona-based Axon (formerly Taser); Motorola Solutions; and the Japanese NEC Corporation, a leading provider of biometric devices for local, state and federal law enforcement, including ICE. Other IJIS members[140] include Northrop Grumman, creator of the LInX information sharing application; IBM, until recently the owner of COPLINK; and BI2 Technologies, a Massachusetts company operating in 47 states with funding from John Ashcroft's The Ashcroft Group[141] that was an early participant in the FBI's 2013 iris pilot program[142] and contracted with the Southwestern Border Sheriff's Association in 2017.[143]

4.3. Palantir's Point of Leverage: California Fusion Centers and Sheriffs

Palantir is a competitor of COPLINK, though it does not have nearly the market share nationally. It has implemented its analytical policing software at the New York Police Department, the Cook County Sheriff's Office in Chicago, the Virginia State Police, the Metropolitan Police Department in Washington, D.C., and a dozen law enforcement agencies in Utah.[144] Palantir also implemented its predictive policing technology in New Orleans for six years, free of charge.[145] However, it has not always been able to get lasting contracts; its NYPD contract and the New Orleans deal were eventually canceled.

Palantir's biggest presence at the state and local level, however, is in California where it has taken a targeted, strategic approach to leverage its recent presence at DHS (ICM and FALCON-SA) to expand into policing and information sharing. Palantir has focused on contracting with law enforcement tied to DHS through fusion centers in the state, as well as LEISI programs in the Los Angeles and San Diego metropolitan areas, and the local agencies connected to all of these centralized policing hubs.

[139] IJIS Institute, "IJIS Institute National Symposium Set for January 20-21, 2016," press release, December 17, 2015, https://cdn.ymaws.com/www.ijis.org/resource/collection/D69CFC9E-624F-4843-A24E-0D9EA22D0439/PR_20151217_AWS_platinum_natl_symp_sponsor.pdf.
[140] For a complete list of IJIS members, see: https://www.ijis.org/page/Member_List.
[141] "BI2 Technologies and The Ashcroft Group Announce Strategic Alliance and Investment Agreement," Business Wire, June 30, 2015, https://www.businesswire.com/news/home/20150630005895/en/BI2%C2%A0Technologies-Ashcroft-Group-Announce-Strategic-Alliance-Investment.
[142] Aliya Sternstein, "Eye on crime: The FBI is building a database of iris scans," Nextgov, June 27, 2012, https://www.nextgov.com/emerging-tech/2012/06/eye-crime-fbi-building-database-iris-scans/56481/.
[143] George Joseph, "The Biometric Frontier," The Intercept, July 8, 2017, https://theintercept.com/2017/07/08/border-sheriffs-iris-surveillance-biometrics/.
[144] Mark Harris, "How Peter Thiel's Secretive Data Company Pushed Into Policing," Wired, August 9, 2017, https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/.
[145] Ali Winston, "New Orleans ends its Palantir predictive policing program," The Verge, March 15, 2018, https://www.theverge.com/2018/3/15/17126174/new-orleans-palantir-predictive-policing-program-end.

Table 7. Palantir software use: LEIS Network and Fusion Centers in California

DHS information sharing modality	LEISI Regional Participant	Local member agencies (in addition to DHS, FBI and other federal partners)	Palantir software funded by
LEIS Network	Automated Regional Justice Information System (ARJIS)[146]	Carlsbad Police Department Chula Vista Police Department Coronado Police Departmental El Cajon Police Departmental Escondido Police Department La Masa Police Department National City Police Department Oceanside Police Department San Diego Police Department San Diego Harbor Police San Diego Sheriff's Department[147]	
LEIS Network/Fusion Center	Los Angeles Sheriff's Department as fiduciary for Joint Regional Intelligence Center[148]	Memorandum of Agreement for Palantir data sharing between: Los Angeles Sheriff's Department Los Angeles Police Department Long Beach Police Department Burbank Police Department Glendale Police Department Torrance Police Department Gardena Police Department Orange County Sheriff's Department Santa Monica Police Department	Homeland Security Urban Areas Security Initiative Grant, distributed through the California Governor's Office of Emergency Services

[146] ARJIS has access to Palantir software, presumably through the San Diego Sheriff's Department and San Diego Law Enforcement Coordination Center. See: Alison Brooks, "Digital Evidence Management and Analysis in the Cloud," IDC Canada Consulting, April 2016, cradpdf.drdc-rddc.gc.ca/PDFS/unc232/p804106_A1b.pdf.
[147] ARJIS Agencies, www.arjis.org/SitePages/ARJISAgencies.aspx.
[148] Contract by and between the County of Los Angeles anf Palantir Technologies Inc. for Software Maintenance and Application Support, accessible at: file.lacounty.gov/SDSInter/bos/supdocs/102501.pdf.

		West Covina Police Department Alhambra Police Department[149] JRIC includes municipal police departments throughout Los Angeles, Riverside, San Bernardino, Santa Barbara, San Luis Obispo and Ventura Counties	
Fusion Center	San Diego County Sheriff's Department for San Diego Law Enforcement Coordination Center[150]	San Diego County Sheriff's Department Imperial County Sheriff's Department California Department of Corrections *Municipal police departments throughout San Diego and Imperial Counties*	Homeland Security Urban Areas Security Initiative Grant, distributed through the California Governor's Office of Emergency Services
Fusion Center	Sacramento County Sheriff's Department on behalf of Central California Intelligence Center[151]	Sacramento County Sheriff's Department Sacramento Police Department California Department of Justice California Highway Patrol Governor's Office of Emergency Services	Homeland Security Urban Areas Security Initiative Grant, distributed through the California Governor's Office of Emergency Services
Fusion Center	Orange County Intelligence Assessment Center	Orange County Sheriff's Department *Municipal police departments throughout Orange County*	
Fusion Center	San Mateo County Sheriff's Office for Northern California Regional Intelligence Center[152]	*Sheriff's departments and municipal police departments throughout Del Norte, Humboldt, Mendocino, Lake, Sonoma, Napa, Marin, San Francisco, Contra Costa, Alameda, San Mateo, Santa Clara, Santa Cruz, San Benito, and Monterey Counties*	Recovery Act Grant from United States Department of Justice - Office of Justice Planning to Combat Criminal Narcotics Activity Stemming from the Southern Border
Principal California Fusion Center	California State Threat Assessment System	California Governor's Office of Emergency Services	

[149] Second Amendment to Memorandum of Agreement between Los Angeles Sheriff's Department and Los Angeles Police Department for Data Sharing between Palantir Instances, 2014, accessible at: https://www.muckrock.com/foi/burbank-3129/palantir-technologies-reports-and-documents-31877/#file-117125.
[150] License and Services Agreement between the County of San Diego, through the Sheriff's Department on behalf of the San Diego Law Enforcement Coordination Center, accessible at: https://www.muckrock.com/foi/california-52/palantir-technologies-reports-and-documents-31876/#file-121759.
[151] County of Sacramento, Request for Exemption to Competitive Bidding Process and Disclosure Statement, April 8, 2014, accessible at: https://www.muckrock.com/foi/california-52/palantir-technologies-reports-and-documents-32440/#file-120256.
[152] Agreement between the County of San Mateo and Palantir Technologies Inc., January 10, 2012, accessible at: https://www.muckrock.com/foi/california-52/palantir-technologies-reports-and-documents-30858/#file-113858.

		California Highway Patrol California Department of Corrections and Rehabilitation California Department of Motor Vehicles California Department of Justice California Department of Public Health County Sheriff's Offices City Police, Fire and Emergency Management Departments	

Source: Diverse contract and procurement documents.

Invoices from the above agencies show that they have spent over USD 50 million on Palantir products since 2009, primarily financed with DHS grants.[153] By implementing its software throughout California's fusion centers and two major LEIS partner organizations in the San Diego and Los Angeles metropolitan regions, Palantir created a certain degree of dependency on the part of other fusion centers and sheriff's departments in the state, and introduced their technology to municipal police through these regional sharing systems. In a 2014 request for Palantir software for the Central California Intelligence Center, the County of Sacramento Sheriff's Department argued:

> The acquisition and utilization of systems from Palantir Technologies has become prevalent throughout the California law enforcement community and is currently the only updated main data base center for the California State Threat Assessment System (STAS) intelligence centers. The Central California Intelligence Center (CCIC) is the only intelligence center within the STAS that currently does not utilize Palantir. In order to maintain connectivity with STAS intelligence centers the CCIC needs to purchase Palantir systems. Palantir is the only unique system that will allow for the CCIC to have connectivity with the other intelligence centers and allow the CCIC/STAS to provide consistent technology for our analyst and law enforcement partners.[154]

The importance of this inter-connectivity was heightened by the adoption of Palantir software for ICE's Integrated Case Management (ICM) system in 2014 and its FALCON-SA analytical software in 2015, which is based on the same Gotham software used by local and state police, and which appears to have cut out the need for the ICEPIC application used for the LEIS Service by establishing a direct interface with Palantir's ICM.[155]

Use of Palantir software does not exclude the use of other software like COPLINK; the two programs co-exist in quite a few law enforcement agencies. The Los Angeles Sheriff's Department, for example, has

[153] Mark Harris, "How Peter Thiel's Secretive Data Company Pushed Into Policing," Wired, August 9, 2017, https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/.
[154] County of Sacramento, Request for Exemption to Competitive Bidding Process and Disclosure Statement, April 8, 2014, accessible at: https://www.muckrock.com/foi/california-52/palantir-technologies-reports-and-documents-32440/#file-120256.
[155] DHS, ICE Office of Acquisition Management, Limited Source Justification for Award ID HSCETC13F00035, May 15, 2018, https://govtribe.com/project/tecs-mod-leiss-and-data-migration.

access to COPLINK, Palantir and LInx, among various other searchable systems,[156] and ARJIS uses both COPLINK[157] and Palantir.[158] Forensic Logic's LEAP Network, with which COPLINK will now be integrated, already has a presence in California. In a testimonial for the company, an Oakland Police Department Senior Command staff member says the software is the "heart and soul of IT" for search, analysis and reporting, and that "we'd be lost without it."[159]

The highest-stakes competition between Palantir and the i2 technology behind COPLINK is at the federal level, where the biggest contracts get awarded. Palantir sued the U.S. Army in 2016 for not opening up its acquisition of the new Distributed Common Ground System-Army (DCGS-A) technology for competitive bids. DCGS-A includes i2 software, and Palantir contended that it offered a commercial product for less. In March 2018, Palantir was awarded the USD 876 million contract with the Department of Defense, together with Raytheon under undisclosed terms.[160]

Alongside its large federal contracts with the Department of Defense, Department of Justice and DHS, Palantir has leveraged DHS funding for fusion centers in California to solidify its presence among local law enforcement and its centrality to DHS and ICE information sharing.

4.4. The "Racist Feedback Loop" in COPLINK and Palantir Algorithms

Both COPLINK and Palantir characterize their software as the future of policing, making use of predictive analytics based on past behaviors, which lends itself to racial profiling and other manifestations of potentially discriminatory statistical analysis. Former New Orleans Police Chief Ronal Serpas said that Palantir software, which was secretly used by the city for six years, "was used to identify potential members of the 3NG, the 39ers, and the 110ers gangs."[161] Palantir touts its Gotham software as providing "human-centric" analysis based on "algorithmic processing" to identify ill-defined "interesting clusters of data."[162]

The network analysis that these programs are based on has also been used to target potential activists, as was the case in Memphis where police used IBM's i2 Analyst's Notebook to map relationships between Black Lives Matter activists.[163] i2 was the first company to buy COPLINK from the University of Arizona's

[156] See, for example: Los Angeles County Sheriff's Department, RFI NUMBER 637-SH, shq.lasdnews.net/shq/contracts/637-SH/RFI-637-SH.pdf; Sacramento County Sheriff's Department, Palantir Exception to Bid Justification, SGT Dan Morrissey #182, www.agendanet.saccounty.net/sirepub/cache/2/004cmduilr122ewhuxoos2kj/564228008142018101451348.PDF.
[157] ARJIS, TACIDS report, https://www.eff.org/files/2013/11/07/11-_tacids_final_report_final.pdf.
[158] ARJIS has access to Palantir software, presumably through the San Diego Sheriff's Department and San Diego Law Enforcement Coordination Center. See: Alison Brooks, "Digital Evidence Management and Analysis in the Cloud," IDC Canada Consulting, April 2016, cradpdf.drdc-rddc.gc.ca/PDFS/unc232/p804106_A1b.pdf.
[159] Forensic Logic, LEAP Network testimonials, https://forensiclogic.com/testimonials/.
[160] Department of Defense Award ID W56KGY18D0003, https://www.usaspending.gov/#/award/66537016.
[161] Ali Winston, "New Orleans ends its Palantir predictive policing program," The Verge, March 15, 2018, https://www.theverge.com/2018/3/15/17126174/new-orleans-palantir-predictive-policing-program-end.
[162] Palantir Gotham, https://www.palantir.com/palantir-gotham/platform/.
[163] Brentin Mock, "Memphis Police Spying on Activists Is Worse Than We Thought," CityLab, July 27, 2018, https://www.citylab.com/equity/2018/07/memphis-police-spying-on-activists-is-worse-than-we-thought/566264/.

Hsinchun Chen, and was later bought by IBM, though the i2 Analyst's Notebook was not part of the COPLINK sale to Forensic Logic.

Simple network analysis may not present any new policing problems, but the algorithms used by programs such as COPLINK and Palantir can reinforce assumptions made by police officers. "While race would never be included as part of the algorithm," writes Andrew Guthrie Ferguson in The Rise of Big Data Policing, "many of the variables (police contacts, prior arrests, gang affiliations) directly correlate with racially discriminatory law enforcement practices."[164] The Stop LAPD Spying Coalition characterizes this as a "racist feedback loop," one that is seen in the LAPD's Operation LASER (Los Angeles Strategic Extraction and Restoration), which uses Palantir software to track "a person's criminal history, gang affiliation, previous detentions, and associations" across divisions. The LAPD uses Palantir software to evaluate data sources including "crime incidents, arrests, field interviews, calls for service, license plate readers, vehicle recovery, and citizen tips," and then targets individuals and places for investigation and intervention.[165]

Another application used by the LAPD for predictive policing, PredPol,[166] was founded by UCLA anthropologist Jeff Brantingham. The program stemmed from Brantingham's research for military applications with funding from a U.S. Army Research Office grant.[167] Statistical research by the Human Rights Data Analysis Group on the policing of drug crimes in Oakland has shown that predictive policing algorithms, specifically those used by PredPol, have resulted in "increasingly disproportionate policing of historically over-policed communities."[168]

Palantir and COPLINK use similar algorithms for their predictive analytics—so similar that in 2011, Palantir settled with i2 for some USD 10 million[169] over intellectual property obtained by Palantir executive Shyam Sankar and others for use in the development of Palantir software. By licensing i2 products through a Florida front company, Sankar allegedly obtained core trade secrets and other confidential information, and violated license terms prohibiting the sharing of proprietary information with a competitor.[170]

---

[164] Andrew Guthrie Ferguson, *The Rise of Big Data Policing*, NYU Press, 2017.
[165] Craig D. Uchida et al., "Los Angeles, California Smart Policing Initiative," Bureau of Justice Assistance, October 2012, newweb.jssinc.org/wp-content/uploads/2014/11/Spotlight-on-Operation-LASER.pdf.
[166] See reference to LASD use of the program (erroneously referred to as PedPol) alongside Palantir, COPLINK and LInX in: Los Angeles County Sheriff's Department, RFI NUMBER 637-SH, shq.lasdnews.net/shq/contracts/637-SH/RFI-637-SH.pdf
[167] Ali Winston and Darwin BondGraham, "From Fallujah to the San Fernando Valley, Police Use Analytics to Target "High-Crime" Areas," Truth-out, March 12, 2014, https://truthout.org/articles/predictive-policing-from-fallujah-to-the-san-fernando-valley-military-grade-software-used-to-wage-wars-abroad-is-making-its-impact-on-americas-streets/.
[168] Kristian Lum and William Isaac, "To predict and serve?" Significance, October 7, 2016, https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x.
[169] Peter Waldman, Lizette Chapman, and Jordan Robertson, "Palantir knows everything about you," Bloomberg, April 19, 2018, https://www.bloomberg.com/features/2018-palantir-peter-thiel/.
[170] United States District Court, Eastern District of Virginia, Civil Action 1:10-CV-00885-LO/JFA, accessible at: https://www.scribd.com/doc/36371667/i2-v-palantir-080910.

5. Feeding the Algorithms: Data Brokers and Social Media Analytics

5.1. Data Brokers and Social Media Analytics

5.1.1. DATA BROKERS

One week after Forensic Logic's purchase of COPLINK from IBM in October 2017, Forensic Logic announced an agreement for data integration with Thomson Reuters CLEAR,[171] which provides data sets for investigative purposes, including utilities data, DMV records, real property data, criminal and court records, arrest records from more than 2,200 facilities, business data, healthcare provider information,[172] live cell phone records, and license plate recognition from contractor Vigilant Solutions.[173] Thomson Reuters CLEAR offers services tailored specifically to law enforcement.

ICE has over USD 46 million in current potential contracts with Thomson Reuters subsidiary West Publishing Corporation for CLEAR services through HSI,[174] in addition to contracts through ERO specifically for access to the license plate reader database[175] (a service that Thomson Reuters contracts through Vigilant Solutions), as well as other multi-million dollar ICE contracts directly with Thomson Reuters through both HSI[176] and ERO.[177] Contracting documents for CLEAR services at HSI specifically require the data broker to be compatible with Palantir's FALCON analytics program and reveals that there is a direct interface between the Thomson Reuters and Palantir software:

> The Government's requirement is that the database must be able to interface with FALCON Palantir systems. West Publishing Corporation's CLEAR program offers a system to system (S2S) connection that merges CLEAR public and proprietary data with Palantir analytical information to narrow in and locate persons and assets of interest.[178]

[171] "Thomson Reuters CLEAR, Forensic Logic/Coplink Plan Data Alliance," Police Magazine, October 19, 2017, https://www.policemag.com/channel/technology/news/2017/10/19/thomson-reuters-clear-forensic-logic-coplink-plan-data-alliance.aspx.
[172] Thomson Reuters CLEAR, https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-brochure.pdf.
[173] Thomson Reuters CLEAR, https://legalsolutions.thomsonreuters.com/law-products/solutions/clear-investigation-software/law-enforcement.
[174] DHS Award ID HSCEMD17F00008, https://www.usaspending.gov/#/award/23831008; DHS Award ID HSCEMD16F00003, https://www.usaspending.gov/#/award/23830679.
[175] DHS Award ID 70CDCR18P00000017, https://www.usaspending.gov/#/award/8288562.
[176] See, for example, DHS Award ID HSCEMD16C00002, https://www.usaspending.gov/#/award/23830675; DHS Award ID HSCEMD15P00091, https://www.usaspending.gov/#/award/23830656; and DHS Award ID HSBP1015P00702, https://www.usaspending.gov/#/award/23779955.
[177] See, for example, DHS Award ID HSCEDM16P00082, https://www.usaspending.gov/#/award/23822745; and DHS Award ID 70CDCR18P00000048, https://www.usaspending.gov/#/award/62503110.
[178] DHS Limited Source Justification for Award ID GS02F0405D, https://www.usaspending.gov/#/award/15631373, accessible at: https://www.mediafire.com/file/y2e3vk65z6v3k6x/LSJ_Final.pdf.

Nlets, the network of state law enforcement agencies that feeds the FBI's NCIC database and has access to ICE data through the LEIS Service and the Palantir ICM system, is also a corporate partner of Thomson Reuters CLEAR.[179]

ICE agents using ICM and FALCON-SA have access to business data provided on a contract basis by Dun & Bradstreet, which like Thomson Reuters has a commercial data integration agreement with Palantir.[180]

5.1.2. SOCIAL MEDIA ANALYTICS

The Privacy Impact Assessment for Palantir's ICM system reveals that "ICM users may directly or indirectly (via a commercial data provider) access public information on the Internet, including social media websites, during the course of investigations and incorporate that information into case documents." This can happen in several ways:

- Ad hoc data entry into Palantir systems of social media information obtained through general surveillance or obtained with subpoenas directly from companies including Facebook.[181]
- Collection and analysis of social media and messaging data from services including Facebook, Whatsapp (owned by Facebook), and Twitter, through the Telecommunications Linking System (TLS) that is a component of Palantir's ICM system. TLS is a commercial product provided by Pen-Link, which currently has a contract potentially worth over USD 10 million with ICE through 2022.[182] Government documents prepared for ICE's contract with Pen-Link specifically mention these and other social media and messaging companies.[183]
- Social network data compiled for analysis by Giant Oak of Arlington, Virginia, which has several contracts with ICE, including one potentially worth more than USD 37 million for "open source/social media data analytics."[184]

Giant Oak President and CEO Gary Shiffman was Chief of Staff at CBP.[185] He is former Managing Director of the Chertoff Group (Michael Chertoff was DHS Secretary under the Bush administration). Shiffman founded Giant Oak in 2009 to support research funded by DARPA, the tech development branch for the Department of Defense.[186]

---

[179] Nlets partners, page accessible at: https://web.archive.org/web/20171006224739/www.nlets.org:80/partnerships/strategic-partner-list.
[180] Palantir, Data and Device Partners, https://www.palantir.com/partnerships/data-providers/.
[181] Facebook, Government Requests for User Data, https://transparency.facebook.com/government-data-requests.
[182] DHS Award ID HSCETC17C00001, https://www.usaspending.gov/#/award/23844564.
[183] DHS Justification and Approval for Other than Full and Open Competition, https://www.deportice.org/the-targets/.
[184] DHS Award ID HSCEMD17D00001, https://www.usaspending.gov/#/award/23830999; DHS Award ID HSCEMD17J00077, https://www.usaspending.gov/#/award/23831339; DHS Award ID 70CMSD18FR0000096, https://www.usaspending.gov/#/award/66685141; DHS Award ID 70CMSD18FR0000173, https://www.usaspending.gov/#/award/67807277; DHS Award ID HSCEMD17J00082, https://www.usaspending.gov/#/award/23831342; DHS Award ID HSCEMD17J00153, https://www.usaspending.gov/#/award/23831407; DHS Award ID HSCEMD17J00034, https://www.usaspending.gov/#/award/23831300; and DHS Award ID HSCEMD17J00031, https://www.usaspending.gov/#/award/23831298. Giant Oak also has a contract with ICE for "data analytics and custom alert services": DHS Award ID HSCEMD14C00002, https://www.usaspending.gov/#/award/23829929;
[185] Giant Oak, Gary Shiffman biography, www.giantoak.com/gary-shiffman/.
[186] 2017 Financial Crime Conference, Gary Shiffman biography, https://www.financialcrimeconference.com/speaker/shiffman-gary/.

5.2. Biometric Collection and Matching

To complement the mountain of biographic and personally identifiable information to be obtained from data brokers, ICE and DHS have placed an emphasis on the development and use of biometrics. There is a large and growing market for biometric collection devices and services, much of that for law enforcement purposes. The Biometrics Research Group estimates that that the global biometrics market will grow to US 35.5 billion by 2020 from its 2015 value of USD 15 billion, and that approximately half of this projected 2020 spending (USD 18 billion and USD 7.5 billion, respectively) will be spent on law enforcement biometrics. Of the estimated USD 18 billion to be spent on law enforcement in 2020, a majority—some USD 15 billion—will be dedicated to automated fingerprint identification systems, and the remaining USD 3 billion on newer technologies including voice, iris and facial recognition.[187]

Due to the biometric sharing agreements in place across U.S. jurisdictions, biometric technologies must be compatible and standardized, and the FBI's CJIS has certification procedures in place for diverse fingerprint and palm print modalities.[188] The FBI also has programs in development for facial recognition[189] and iris scanning[190] technologies, and these biometric markers are already part of the NGI database housed at CJIS facilities in West Virginia, which is interoperable with the Pentagon and DHS biometric databases.

Research on these technologies is conducted by the Biometric Center of Excellence (BCOE) at CJIS, which partners with the following institutions[191]:

- Department of Defense
- Department of State
- Department of Homeland Security
- National Institute of Justice (NIJ) of the Department of Justice
- National Institute of Standards and Technology (NIST)
- State and local law enforcement
- West Virginia University leads a research agreement with 33 academic institutions including Carnegie Mellon, Notre Dame and Syracuse[192] and has an agreement with NGI biometric database contractor IDEMIA (see below).[193]

---

[187] Rawlson O'Neil King, "Special Report: Biometrics in Law Enforcement," Biometrics Research Group, 2017, https://www.biometricupdate.com/wp-content/uploads/2017/08/special-report-biometrics-in-law-enforcement.pdf.
[188] Products certified by modality are listed by the FBI at: https://www.fbibiospecs.cjis.gov/Certifications.
[189] FBI, Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.
[190] FBI, Privacy Impact Assessment for the FBI Iris Pilot, April 21, 2017, https://www.fbi.gov/file-repository/pia-fbi-ngi-iris-pilot.pdf/view.
[191] FBI Biometric Center of Excellence, Partners, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence/partners.
[192] Sandra Gittlen, "The FBI's Biometric Center of Excellence Peers into Future of ID Technology," FedTech, August 2, 2016, https://fedtechmagazine.com/article/2016/08/fbis-biometric-center-excellence-peers-future-id-technology.
[193] Charles Young, "IDEMIA National Security Solutions: Leading innovation and opportunity in Morgantown," WVNews, July 8, 2018, https://www.wvnews.com/news/wvnews/idemia-national-security-solutions-leading-innovation-and-opportunity-in-morgantown/article_e60904f9-f895-5b2b-ba99-8df9c2e9e985.html.

BCOE research covers modalities including facial recognition, palm print, iris scan, voice recognition, fingerprint and DNA.[194]

5.2.1. A GROWING BIOMETRICS MARKET IN U.S. IMMIGRATION ENFORCEMENT

There are some 145 companies certified by CJIS for fingerprint and palm print technologies,[195] and a plethora of companies peddling facial recognition and iris scanning technologies to law enforcement across the country, including Amazon, which has sold its facial Rekognition technology to the Washington County Sheriff's Office[196] outside Portland, Oregon, and the Orlando Police Department.[197] Amazon Rekognition is, of course, hosted on the AWS cloud AWS.[198]

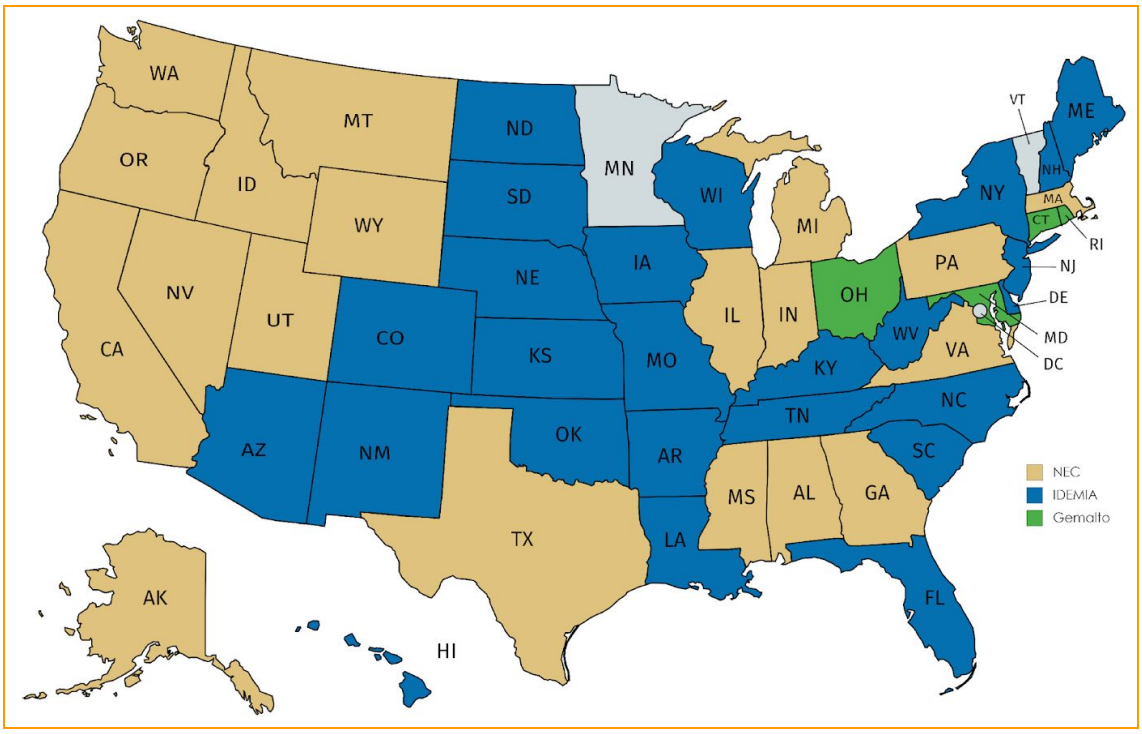
However, the biometrics market is dominated by three companies, the result of a flurry of recent mergers among the largest international players:

- Gemalto (Netherlands), subsidiary of French company Thales, operating through Gemalto Inc. in Austin, Texas
- NEC Corporation (Japan), operating through NEC Corporation of America in Irving, Texas
- IDEMIA (France), formerly OT-Morpho, majority-owned by Boston private equity firm Advent International and operating through MorphTrak in Anaheim, California

These companies have a presence in the development and operation of biometrics systems at every level of U.S. law enforcement. Figure 12 shows how contracting with state law enforcement agencies for Automated Fingerprint Identification Systems (AFIS) is effectively split between the three companies.

[194] FBI Biometric Center of Excellence, Modalities, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence/modalities.
[195] Products certified by modality are listed by the FBI at: https://www.fbibiospecs.cjis.gov/Certifications.
[196] ACLU of Oregon, "Amazon Teams Up With Law Enforcement to Deploy Dangerous New Face Recognition Technology," May 22, 2018, https://aclu-or.org/en/news/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology-heres-how-its.
[197] Diamond Naga Siu, "Turns out Orlando won't stop using Amazon's facial recognition software," Mashable, July 13, 2018, https://mashable.com/2018/07/13/orlando-rekognition-amazon-surveillance/#piDTXYjsMmqg.
[198] AWS, Amazon Rekognition, https://aws.amazon.com/rekognition/,

Figure 12. Automated Fingerprint Identification Systems (AFIS) contracting by state law enforcement agency, 2014



*Source: Empower LLC image, data from U.S. DOJ National Institute of Justice, Latent Fingerprint Interoperability Survey, August 2014. *Original survey data included MorphoTrak (since bought by IDEMIA) and 3M Cogent (since bought by Gemalto).*

In keeping with Figure 12 (above), AZLink CIO Bill Kalaf[199] noted in 2010 that "Sagem Morpho-Morpho Division [now IDEMIA] is the sole source for biometrics identification products for Arizona."[200] The company also has law enforcement contracts for facial recognition: subsidiary MorphoTrak launched a statewide mugshot facial recognition system in Hawaii in 2015 after the program had been used by the Honolulu Police Department.[201]

The same survey found, based on less comprehensive data, that local law enforcement AFIS contracts throughout the country were awarded as follows, primarily to the same three companies:

[199] *Bill Kalaf LinkedIn profile*, https://www.linkedin.com/in/bill-kalaf/.
[200] *William M. Kalaf, "Arizona law enforcement biometrics identification and information sharing technology framework," master's thesis, Naval Postgraduate School, March 2010,* https://calhoun.nps.edu/bitstream/handle/10945/5370/10Mar_Kalaf.pdf?sequence=1&isAllowed=y.
[201] "Honolulu PD Facial Recognition System Expands for Statewide Use," Yahoo Finance, January 28, 2015 https://finance.yahoo.com/news/honolulu-pd-facial-recognition-system-144000973.html.

Table 8. Automated Fingerprint Identification Systems (AFIS) contracting by local law enforcement agency, 2014

Company	Responding local law enforcement agencies
IDEMIA (MorphoTrak)	26
NEC	21
Gemalto (3M Cogent)	13
AFIX Technologies	12
SPEX Forensics	9

Source: U.S. DOJ National Institute of Justice, Latent Fingerprint Interoperability Survey, August 2014

Since January 2018, the Los Angeles County Sheriff's Department—a key Palantir client that is part of the DHS LEIS Initiative and tied to the regional JRIC fusion center—has been using NEC's Integra ID 5 biometric database, which supports fingerprint, palm print, face and iris modalities, and also has voice recognition capabilities. The Sheriff Department's NEC system interfaces with the FBI's NGI biometric database.[202]

Elsewhere in California, the San Francisco Police Department (SFPD) uses Gemalto's COGENT Automated Biometric Identification System (ABIS). The SFPD system's manager notes that the Gemalto LiveScan software "captures the palms, the fingerprints, the demographics and the photograph at the time of booking and puts it all in one package, and sends it not only to our system but all the way through to all the state and federal systems, and it synchronizes all of the data simultaneously."[203]

In 2015, the Electronic Frontier Foundation and MuckRock coordinated a mass submission of public records requests to municipalities across the country regarding mobile biometric technology used by law enforcement in the field. Responses by local government were limited, but included several of the largest cities in the country. The two most widely-used devices for mobile fingerprint capture were Gemalto's BlueCheck MobileID and Mobile Ident II and the DataWorks Plus RapidID fingerprint scanner.[204] DataWorks Plus is based in Greenville, South Carolina.

At the federal level, NEC Corporation currently provides face and iris matching algorithms for the DHS biometric database (IDENT) and will continue to do so for its replacement (HART) while Gemalto will continue to provide fingerprint matching algorithms.[205] At the 2018 DHS Biometric Technology Rally, NEC

[202] NEC Corporation, "Los Angeles County Sheriff's Department's New Multimodal Identification Biometric Solution Goes Live," press release, March 15, 2018, https://www.nec.com/en/press/201803/global_20180315_03.html.
[203] Gemalto, "San Francisco Police Department and the Gemalto Cogent ABIS," https://www.gemalto.com/govt/customer-cases/sfpd.
[204] Documented responses to all public records requests are available on the campaign page: MuckRock, Street Level Surveillance: Biometrics FOIA campaign, https://www.muckrock.com/foi/list/?projects=11. For an analysis of responses in California, see: Dave Mass, "California Cops Are Using These Biometric Gadgets in the Field," Electronic Frontier Foundation, November 4, 2015, https://www.eff.org/deeplinks/2015/11/how-california-cops-use-mobile-biometric-tech-field.
[205] Chris Burt, "Northrup Grumman progressing on new DHS biometric system," Biometric Update, May 8, 2018, https://www.biometricupdate.com/201805/northrup-grumman-progressing-on-new-dhs-biometric-system.

and Gemalto scored the highest on facial recognition tests.[206] In another NIST competition in March 2018, IDEMIA won the top spot for facial recognition algorithms.[207] IDEMIA has a facial recognition contract with the Department of State (a contract for which NEC Corporation and Microsoft also competed).[208]

Meanwhile, IDEMIA provides the algorithms for finger and palm prints for the FBI's NGI biometric database,[209] as well as facial recognition and iris matching.[210] An early predecessor of the company, Rockwell Autonetics, developed AFIS in 1974 for the FBI Automated Fingerprint Identification System (AFIS), which handles an average of 230,000 searches daily.[211] IDEMIA provides cloud services for its Automated Fingerprint Identification System (AFIS) through MorphoCloud, hosted by Microsoft Azure Government.[212]

ICE agents in the field, who collect much of the information that goes into IDENT and HART, use the NEC NeoScan fingerprint device,[213] as well as a mobile app called EDDIE developed by Wexler Technical Solutions.[214] CBP's new Biometric Entry-Exit program makes use of NEC's NeoFace facial recognition technology.[215]

IDEMIA makes driver's licenses in 42 states, including many REAL ID-compliant cards, with an estimated 80 percent market share nationally, and produces U.S. passports and passport cards, in addition to screening the identities of U.S. passport and visa applicants.[216]

IDEMIA also manages biometrics for Mexico's National Electoral Institute (INE). In December 2016, the company (at the time Safran Identity and Security, recently merged with Morpho) won a five-year contract to continue managing INE fingerprint and facial recognition services, which it has supported since 2005.[217] This is a separate system from that which the U.S. government is installing with contractor CSRA at detention centers for Mexico's National Migration Institute, but biometric sharing between the two countries may eventually implicate INE data.

---

[206] Sara Friedman, "Face off: Biometric rally tests facial recognition algorithms," GCN, July 3, 2018, https://gcn.com/articles/2018/07/03/biometric-rally.aspx.
[207] Chris Burt, "IDEMIA claims top spot in two categories at NIST Face Recognition Vendor Test," Biometric Update, March 22, 2018, https://www.biometricupdate.com/201803/idemia-claims-top-spot-in-two-categories-at-nist-face-recognition-vendor-test.
[208] U.S. Federal Business Opportunities, Solicitation No. 1045815087-1, Department of State, "Notice of Intent-Facial Recognition," https://www.fbo.gov/index?s=opportunity&mode=form&id=175e4f707e6ae5ea8bd826b4b5129554&tab=core&_cview=0.
[209] IDEMIA, "Biometric Technology Supplied by MorphoTrak for FBI NGI to Transform Crime-Solving," press release, July 9, 2013, https://www.morpho.com/en/media/biometric-technology-supplied-morphotrak-fbi-ngi-transform-crime-solving-20130709. See DOJ Award ID DJF161200P0006699, https://www.usaspending.gov/#/award/13094503.
[210] DOJ Award ID DJF161200P0006699, https://www.usaspending.gov/#/award/13094503.
[211] IDEMIA, Public Security, https://www.morpho.com/en/mobile-and-automated-systems-improve-public-security.
[212] IDEMIA, MorphoCloud, www.morphocloud.us/.
[213] DHS Award ID HSCETE17J00357, https://www.usaspending.gov/#/award/23851115. See also: NEC, Current Support, https://www.necam.com/AdvancedRecognitionSystems/FederalGovernment/Sectors/BorderTransportationSecurity/.
[214] Bianca Spinosa, "EDDIE, ICE and apps," FCW, May 28, 2015, https://fcw.com/articles/2015/05/28/eddie-ice-and-apps.aspx.
[215] NEC, Current Support, https://www.necam.com/AdvancedRecognitionSystems/FederalGovernment/Sectors/BorderTransportationSecurity/.
[216] *IDEMIA, "MorphoTrust Solutions Produce North American driver licenses," April 24, 2014, https://www.morpho.com/en/media/morphotrust-solutions-produce-north-american-driver-licenses-20140424. See also: Twila Brase and Matt Flanders, "Exposing IDEMIA: The Push for National Biometric IDs in America," Citizens´ Council for Health Freedom, February 2018, www.cchfreedom.org/pr/Policy%20Insights%20-%20Idemia.pdf.*
[217] IDEMIA, "Our US Companies," https://usa.morpho.com/morpho-usa.

5.2.2. IRIS SCANNING ON THE BORDER

Most biometric collection by law enforcement consists of various types of fingerprinting. Of 79 local law enforcement respondents to the same 2014 DOJ survey cited above, only two reported that they could enroll irises (see "other" in Table 9).

Table 9. Biometric modalities at local and state law enforcement agencies, 2014 survey

Response	State	Local
Number of responses	*48*	*79*
Tenprint rolled fingerprints	48	78
Tenprint slap, flat, or plain fingerprints	47	77
Mobile ID fingerprints	24	32
Palm prints	45	72
Plantar prints	9	15
Latent fingerprints	46	79
Latent palm prints	44	74
Unidentified latent prints	43	79
Mugshots	33	43
Signatures	18	8
Other	9	4

Source: U.S. DOJ National Institute of Justice, Latent Fingerprint Interoperability Survey, August 2014.

The number of state and local agencies with iris capabilities has likely expanded since 2014, but it is still only a supplementary biometric technology for law enforcement. That said, it may be playing an increasingly important role in immigration enforcement. In 2017, a Massachusetts-based company called BI2 Technologies agreed to provide its iris scanner system to all 31 member agencies of the Southwestern Border Sheriffs' Coalition.[218]

BI2 has been collaborating with the FBI since 2012, when it gave 12,000 iris images to the agency's NGI biometric database, shortly before the official start of the agency's iris pilot program.[219] The FBI now retains more than 450,000 iris images and "relies on its partnerships with local, state, tribal, and federal

[218] "Southwestern Border Sheriffs' Coalition (SBSC) to immediately begin improving the biometric identification capabilities of the 31 Sheriffs' Offices along the U.S. and Mexico Border to increase border security and combat criminal activity," Business Wire, April 6, 2017, https://www.businesswire.com/news/home/20170406006132/en/Southwestern-Border-Sheriffs%E2%80%99-Coalition-SBSC-immediately-improving.

[219] Aliya Sternstein, "Eye on crime: The FBI is building a database of iris scans," Nextgov, June 27, 2012, https://www.nextgov.com/emerging-tech/2012/06/eye-crime-fbi-building-database-iris-scans/56481/.

agencies to collaboratively choose new technologies that would best serve the law enforcement and criminal justice communities"—in other words, it relies on private companies such as BI2 that contract with local and state law enforcement agencies.[220] The FBI does not specify which partners contribute to the database, but BI2 has a private database in San Antonio, housed by a third-party vendor, which John Leonard, senior vice president of BI2, claims is the largest of its kind in North America.[221] The company collaborates with local law enforcement agencies in 47 states—including the Los Angeles Sheriff's Department and the Washington, D.C. Department of Corrections—and claims that "more than 2,100 of the nation's 3,000 Sheriffs have asked to join the network."[222]

BI2 received funding in 2015 from TAG Holdings, a company run by John Ashcroft.[223] BI2 has also had a presence on the other side of the U.S.-Mexico border. In 2007, the company signed an agreement with the Asociación de Maquiladoras in Juárez, Chihuahua, to provide maquila employers with iris-scanning technologies to screen employees.[224] Also in 2007, BI2 signed an agreement with Cosmocolor, a provider of driver's licenses in several Mexican states, granting Cosmocolor exclusive distribution rights of BI2 products in Mexico, Central and South America.[225] The President of Cosmocolor is Jorge Kahwagi Gastine, the former head of the CANACINTRA business association during the corrupt presidency of Carlos Salinas de Gortari. Kahwagi is close to Carlos Slim,[226] the richest person in Mexico, who made his fortune off the privatization of the state telecommunications company during Salinas De Gortari's presidency.

As early as June 2012 the FBI selected IDEMIA (at the time MorphoTrust) for its NGI database capture system (the company had long been a contractor for the agency's biometric, primarily fingerprint-oriented database). The company established a West Virginia office in Morgantown in 2015, taking advantage of the company's research agreement with West Virginia University and its AFIS services for the West Virginia State Police.[227] The Morgantown office has greatly expanded[228] since the FBI awarded IDEMIA a 2016 contract in excess of USD 3 million dollars for "NGI MorphoTrust ABIS Face and ABIS Iris."[229] The current primary contractor for the NGI database is Leidos, based in Northern Virginia.[230]

---

[220] FBI, Privacy Impact Assessment for the FBI Iris Pilot, April 21, 2017, https://www.fbi.gov/file-repository/pia-fbi-ngi-iris-pilot.pdf/view.
[221] George Joseph, "The Biometric Frontier," The Intercept, July 8, 2017, https://theintercept.com/2017/07/08/border-sheriffs-iris-surveillance-biometrics/.
[222] BI2 Technologies, About, bi2technologies.com/about.
[223] TAG Holdings, Portfolio, tagholdings.com/portfolio-2/.
[224] "BI2 Technologies and Asociacion de Maquiladoras, A.C. announce agreement to implement Iscientia," Business Wire, July 25, 2007, https://www.businesswire.com/news/home/20070725005853/en/BI2-Technologies-Asociacion-de-Maquiladoras-A.C.-announce.
[225] "Cosmocolor S.A. de C.V. and BI2 Technologies, LLC announce exclusive agreement to offer BI2 Technologies, LLC iris biometric solutions in Mexico, Central and South America," Business Wire, July 30 2007, https://www.businesswire.com/news/home/20070730005698/en/Cosmocolor-S.A.-de-C.V.-BI2-Technologies-LLC.
[226] Rafael Martínez, "Un orgullo ser mexicano y tener raíces libanesas, señala Jorge Kahwagi Gastine," Crónica, November 28, 2017, www.cronica.com.mx/notas/2017/1054370.html.
[227] IDEMIA, "West Virginia Department of Commerce Welcomes MorphoTrak to West Virginia," September 21, 2015, https://www.morpho.com/en/media/west-virginia-department-commerce-welcomes-morphotrak-west-virginia-20150921.
[228] Charles Young, "IDEMIA National Security Solutions: Leading innovation and opportunity in Morgantown," WVNews, July 8, 2018, https://www.wvnews.com/news/wvnews/idemia-national-security-solutions-leading-innovation-and-opportunity-in-morgantown/article_e60904f9-f895-5b2b-ba99-8df9c2e9e985.html.
[229] *DOJ Award ID DJF161200P0006699*, https://www.usaspending.gov/#/award/13094503.
[230] *Leidos, "Leveraging Agile for FBI's Next Generation Identification System,"* https://www.leidos.com/sites/g/files/zoouby166/files/2018-08/cs-leveraging-agile-for-fbi-s-next-generation-identification-system-leidos-2018.pdf.

6. Conclusions

Recent changes in policy and contracting at ICE have heightened the importance of two key tech companies: Amazon, as the primary cloud service provider for the agency, and Palantir, as a provider of case management that can be integrated with key DHS fusion centers and local and state law enforcement agencies.

Forensic Logic's 2017 purchase of COPLINK, and the integration of that program with its LEAP Network, represents a major consolidation of software that provides the basis for most information sharing between DHS and local and state law enforcement—software that was developed by the University of Arizona with DHS funding. Palantir is gaining ground on COPLINK as a competitor, but the two programs are often used in tandem.

Both Forensic Logic's COPLINK and Palantir have commercial interface agreements in place with data broker Thomson Reuters, which also provides diverse data sets of personally identifiable information directly to ICE through a series multi-million dollar contracts.

ICE has considerable access to Facebook and its subsidiary Whatsapp, as well as other social media, both directly, through surveillance and subpoenas, and indirectly, through data brokers like Giant Oak. Palantir Chairman Peter Thiel sits on the Facebook board of directors, and Palantir CIO Arvind KC is former Director of IT at Facebook.

Emergent facial recognition technology by companies including Amazon and Facebook may soon provide specialized capabilities to complement market leaders NEC, Gemalto, and IDEMIA, which provide the biometric technologies that power the massive interoperable biometric databases at DHS, the FBI and the Department of Defense. In conjunction with the Department of State, these agencies have biometric information sharing capabilities with countries including Mexico, El Salvador, Guatemala, Honduras, the Dominican Republic, Jamaica and the Bahamas, even funding a biometric collection system by contractor CSRA (General Dynamics) for the collection of biometric data from individuals jailed by Mexico's National Migration Institute.

The private contractors that develop and maintain person-centric data systems supporting discriminatory, algorithm-driven immigration enforcement must be held accountable for their targeting of affected populations, as must the cloud service providers on which these systems increasingly live.

Annex 1. Company Profile: Palantir Technologies, Inc.

Palantir was founded in 2004 by former PayPal executive Peter Thiel, along with Alex Karp, Joe Lonsdale, and Stephen Cohen, all of whom studied at Stanford University.

> Palantir Technologies Inc. develops and builds data fusion platforms for public institutions, commercial enterprises, and non-profit organizations worldwide. The company offers Palantir Gotham, a platform that integrates, manages, secures, and analyzes enterprise data; and Palantir Metropolis, a platform that integrates, enriches, models, and analyzes quantitative data. It provides solutions in the areas of anti-fraud, capital market, case management, crisis response, cyber security, defense, disaster preparedness, disease response, healthcare delivery, insider threat, insurance analytics, intelligence, law enforcement, legal intelligence, pharmaceutical research and development, and custom aspects. The company was incorporated in 2003 and is based in Palo Alto, California.[231]
>
> Palantir Technologies had approximately 1,639 employees as of 2016.[232]

AWS CLOUD SERVICES

In a June 2018 letter to Jeff Bezos, Amazon employees pointed out that Palantir uses AWS for cloud hosting, citing a forum post by Palantir CIO and former Facebook Director if IT[233] Arvind KC that stated, "At Palantir, we moved all on prem servers to the cloud (AWS)."[234] As it concerns the Palantir contract with DHS for the ICM system, government documents cited in this report support this claim. Palantir's broader use of AWS suggests that Amazon may also provide cloud hosting for state and local law enforcement information sharing partners that contract with Palantir.

FUNDING AND VALUATION

Palantir is valued at about 20 USD billion (though some shareholders place its value at less than half that [235]) with an estimated USD 3.5 billion in bookings for 2017, 40 to 50 percent of this coming from government contracts.[236] The co-founders are significant shareholders: in 2013 Chairman Peter Thiel was the largest shareholder with slightly over 10 percent of ownership, followed by CEO Alex Karp[237]). The

[231] S&P Capital IQ.
[232] S&P Capital IQ.
[233] Arvind KC LinkedIn profile, https://www.linkedin.com/in/arvindkc/.
[234] Post on Pulse by Palantir CIO "Arvind KC," referenced in Amazon employees letter to Jeff Bezos, https://www.pulse.qa/lfdetailedview/how-did-you-make-your-transition-to-the-cloud-what-worked-and-what-didn-t-work/.
[235] Peter Waldman, Lizette Chapman and Jordan Robertson, "Palantir Knows Everything About You," Bloomberg, April 19, 2018, https://www.bloomberg.com/features/2018-palantir-peter-thiel/.
[236] SharesPost Palantir company report, https://sharespost.com/downloads/SharesPost_Palantir_Company_Report.pdf.
[237] Andy Greenberg and Ryan Mac, "How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut," Forbes, September 2, 2013, https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/#e67b7e377852.

company has undertaken a number of private funding rounds. One of the first sources of outside funding was In-Q-Tel, a company that invests in tech companies on behalf of the CIA.[238]

Figure 13. Palantir funding rounds

Date	Amount	Share Class	Post Money Valuation	Key Investors
Jan. 2006	$142,500	Series A	$7MM	Undisclosed investors
Nov. 2006	$10.84MM	Series B	$35.08MM	In-Q-Tel
Feb. 2008	$45.4MM	Series C	$400MM	In-Q-Tel, Reed Elsevier Ventures
Jun. 2010	$97.4MM	Series D	$730MM	Founders Fund, Glynn Capital Management, Ulu Ventures
Apr. 2011	$162MM	Series E	$1.2B	Undisclosed investors
Aug. 2011	$88.3MM	Series F	$1.67B	Western Technology Investment, Tiger Global Management
May 2012	$178.06MM	Series G	$2.5B	Morgan Stanley, Sozo Ventures, 137 Ventures
Sep. 2013	$122.86MM	Series H	$4.03B	Broad Beach Ventures and several individual investors
Dec. 2013	$150MM	Series H1	$4.93B	Broad Beach Ventures and several individual investors
Sep. 2014	$635.71MM	Series I	$9.2B	BlackRock, MicroVenture marketplace, GSV Ventures
Jul. 2015	$400MM	Series J	$15.35B	Undisclosed investors
Dec. 2015	$879.83MM	Series K	$20.4B	TJNS Capital, Nima Capital, Dover Madison Capital Management

Source: SharesPost Palantir company report, https://sharespost.com/downloads/SharesPost_Palantir_Company_Report.pdf.

[238] Rick E. Yannuzzi, "In-Q-Tel: A New Partnership Between the CIA and the Private Sector," https://www.cia.gov/library/publications/intelligence-history/in-q-tel.

Table 10. Palantir board of directors

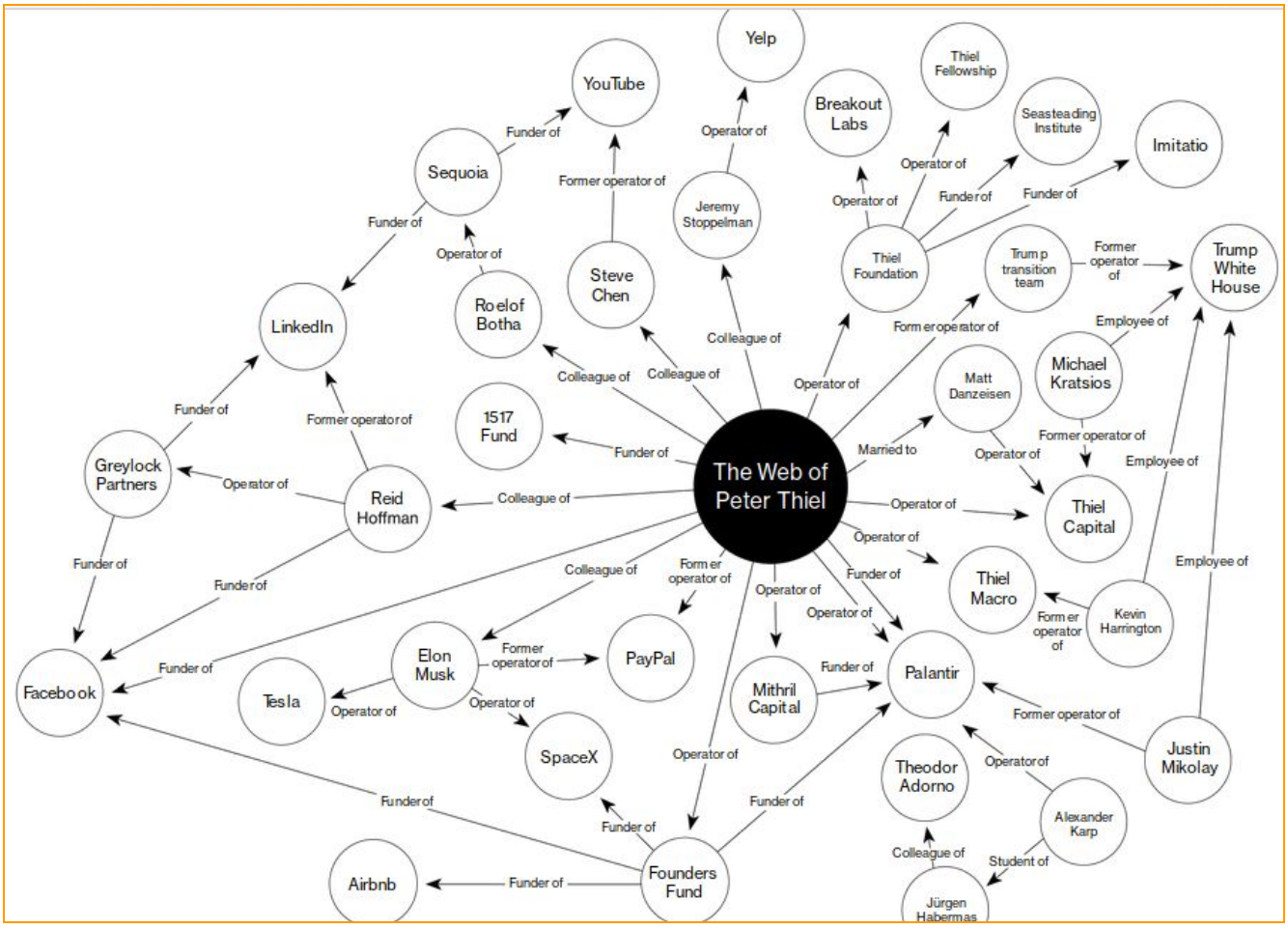
Peter Thiel Co-Founder and Chairman	Co-founder of PayPal Co-founder of Mithril Capital Management Co-founder and Partner at Founders Fund Co-Founder and Partner at Valar Ventures Founder of Clarium Capital Founder of Thiel Capital Facebook board member and early investor Donated 1.25 million to Trump campaign in October 2016[239] Attended meeting with Donald Trump and other tech executives in December 2016[240] Attended private dinner with Donald Trump and Oracle CEO Safra Catz in April 2018[241] Stanford University (JD, 1992)
Alex Karp Co-Founder and CEO	Board member of The Economist[242] Attended meeting with Donald Trump and other tech executives in December 2016[243] Stanford University classmate of Peter Thiel (Law) Expressed opposition to Donald Trump's planned immigration policies in 2015[244]
Stephen Cohen Co-Founder and External Vice President	Stanford University (BSc, Computer Science, 2005)
Adam Ross Co-Founder	Chairman and Chief Executive Officer of Goldcrest Investments Stanford University (BA, 1995) University of Texas (JD, 1998) Took the place of former Palantir CTO and Co-Founder Nathan Gettings

[239] Jessica Guynn, "Mark Zuckerberg defends Peter Thiel's $1.25M Trump donation," USA Today, October 19, 2016, https://www.usatoday.com/story/tech/news/2016/10/19/mark-zuckerberg-defends-peter-thiels-125-million-donald-trump-donation/92426698/.
[240] Nikhil Sonnad, "The seating chart at Trump's table of tech giants," Quartz, December 24, 2016, https://qz.com/863437/who-was-at-donald-trumps-tech-meeting/.
[241] "Oracle's CEO Might Have Given Trump Another Reason to Slam Amazon," Fortune, April 5, 2018, fortune.com/2018/04/05/safra-catz-donald-trump-oracle-amazon/.
[242] The Economist Group, Directors, www.economistgroup.com/results_and_governance/board.html.
[243] Nikhil Sonnad, "The seating chart at Trump's table of tech giants," Quartz, December 24, 2016, https://qz.com/863437/who-was-at-donald-trumps-tech-meeting/.
[244] YouTube video, https://www.youtube.com/watch?v=fnh5ImJCfos.

Table 11. Palantir key advisors

Bryan Cunningham Senior Counsel and Member of Advisory Board	Partner at Cunningham Levy Muse Founding Director of UC–Irvine Cybersecurity Policy & Research Institute Senior Adviser for The Chertoff Group (Michael Chertoff was DHS Secretary in second Bush Administration) Served six years in the Clinton Administration, as a senior CIA officer and federal prosecutor Deputy Legal Adviser to then-National Security Advisor Condoleezza Rice Drafted significant portions of the Homeland Security Act and related legislation, helping to shepherd them through Congress
Michael Hurley Member of Advisory Board	President of Team 3i LLC Advised the 9/11 Commission and their Homeland Security Project at the Bipartisan Policy Center Former Special Advisor, Nuclear Threat Initiative Former Special Advisor, U.S. State Department Former Senior Counsel and Team Leader, 9/11 Commission Former CIA senior operations officer and manager

Figure 14. Peter Thiel relationships



Source: Image by Dorothy Gambrell for Bloomberg[245]

[245] Peter Waldman, Lizette Chapman and Jordan Robertson, "Palantir Knows Everything About You," Bloomberg, April 19, 2018, https://www.bloomberg.com/features/2018-palantir-peter-thiel/.

Annex 2. Amazon Board of Directors and Top Shareholders

Table 12. Amazon.com, Inc. (NASDAQ:AMZN) board of directors

Jeffrey P. Bezos Chairman of the Board, President and CEO	Founded Amazon in 1994 and has been Chief Executive Officer since May 1996. President from founding until June 1999 and again from October 2000 to the present.
Tom A. Alberg Director since June 1996	Managing director of Madrona Venture Group, LLC, a venture capital firm, since September 1999, and a principal in Madrona Investment Group, LLC, a private investment firm, since January 1996. Prior to co-founding Madrona Investment Group, served as president of LIN Broadcasting Corporation, Executive Vice President of McCaw Cellular Communications, Inc., and Executive Vice President of AT&T Wireless Services. Previously, he was chair of the Executive Committee and Partner at Perkins Coie, the Northwest's largest law firm. Director of Impinj, Inc. since September 2000.
Jamie S. Gorelick Director since February 2012	Partner with the law firm Wilmer Cutler Pickering Hale and Dorr LLP since July 2003. Has held numerous positions in the U.S. government, serving as Deputy Attorney General of the United States, General Counsel of the Department of Defense, Assistant to the Secretary of Energy, and a member of the bipartisan National Commission on Terrorist Threats Upon the United States. Served as a director of VeriSign, Inc. since January 2015, a director of United Technologies Corporation from February 2000 to December 2014, and a director of Schlumberger Limited from April 2002 to June 2010.
Daniel P. Huttenlocher Director since September 2016	Dean and Vice Provost, Cornell Tech at Cornell University since 2012, and has worked for Cornell University since 1988 in various positions. Director of Corning Incorporated since February 2015.
Judith A. McGrath Director since July 2014	Senior advisor to Astronauts Wanted * No experience necessary, a multimedia joint venture that Ms. McGrath formed with Sony Music Entertainment, and served as President of Astronauts Wanted from June 2013 to March of 2018. The company is currently a subsidiary of Sony Pictures Television. Chair and Chief Executive Officer of MTV Networks Entertainment Group worldwide, a division of Viacom, Inc., including Comedy Central and Nickelodeon, from July 2004 until May 2011.
Jonathan J. Rubinstein Director since December 2010	Co-CEO of Bridgewater Associates, LP, a global investment management firm, from May 2016 to April 2017. Previously Senior Vice President, Product Innovation, for the Personal Systems Group at the Hewlett-Packard Company (HP), a multinational information technology company,

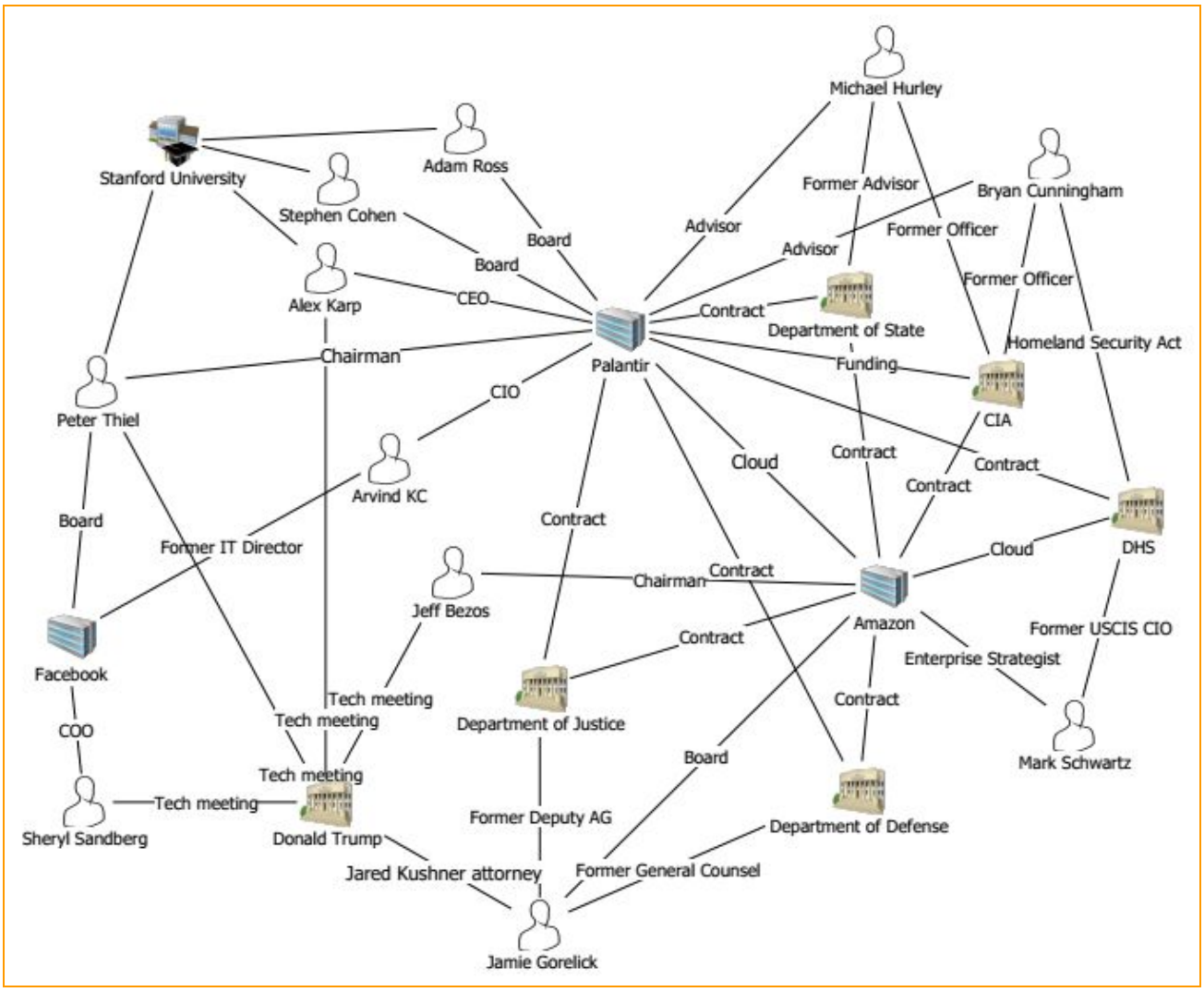
	from July 2011 to January 2012, and served as Senior Vice President and General Manager, Palm Global Business Unit, at HP from July 2010 to July 2011. Chief Executive Officer and President of Palm, Inc., a smartphone manufacturer, from June 2009 until its acquisition by HP in July 2010, and Chairman of the Board of Palm, Inc. from October 2007 through the acquisition. Prior to joining Palm, Senior Vice President at Apple Inc., also serving as the General Manager of the iPod Division. Director of Qualcomm Incorporated from May 2013 to May 2016.
Thomas O. Ryder Director since November 2002	Chairman of the Reader's Digest Association, Inc. from April 1998 to December 2006, and was Chief Executive Officer from April 1998 to December 2005. From 1984 to 1998, worked in several roles at American Express, including as President of American Express Travel Related Services International. Director of Interval Leisure Group, Inc. since May 2016. Director of RPX Corporation from December 2009 to June 2017. Director of Quad/Graphics, Inc. from July 2010 to May 2017. Director of Starwood Hotels & Resorts Worldwide, Inc. from April 2001 to September 2016. Chairman of the Board of Directors at Virgin Mobile USA, Inc. from October 2007 to November 2009.
Patricia Q. Stonesifer Director since February 1997	President and CEO of Martha's Table, a non-profit, since April 2013. Chair of the Board of Regents of the Smithsonian Institution from January 2009 to January 2012 and as Vice Chair from January 2012 to January 2013. From September 2008 to January 2012, senior advisor to the Bill and Melinda Gates Foundation, where she was Chief Executive Officer from January 2006 to September 2008 and President and Co-chair from June 1997 to January 2006. From 1988 to 1997, worked in many roles at Microsoft Corporation, including as a Senior Vice President of the Interactive Media Division, and also served as the Chairwoman of the Gates Learning Foundation from 1997 to 1999.
Wendell P. Weeks Director since February 2016	Chief Executive Officer of Corning Incorporated, a glass and materials science innovator, since April 2005; Chairman of the board of directors since April 2007; and President since December 2010. Mr. Weeks has served as a director of Merck & Co., Inc. since February 2004.

Table 13. Top 20 Amazon.com, Inc. (NASDAQ:AMZN) shareholders

Shareholder	Percent of common stock (USD)	Stock value (mm USD)
Bezos, Jeffrey P.	16.174	148,479.2
The Vanguard Group, Inc.	5.963	54,740.1
BlackRock, Inc.	5.208	47,813.1
FMR LLC	3.487	32,009.9
Capital Research and Management Company	3.484	31,982.4
T. Rowe Price Group, Inc.	3.278	30,097.2
State Street Global Advisors, Inc.	3.122	28,661.4
Baillie Gifford & Co.	1.113	10,216.2
Northern Trust Global Investments	0.965	8,860.9
Geode Capital Management, LLC	0.947	8,693.2
Invesco Capital Management, LLC	0.857	7,865.1
Norges Bank Investment Mangement	0.830	7,617.1
BNY Mellon Asset Management	0.815	7,484.2
Teachers Insurance and Annuity Association of America - College Retirement Equities Fund	0.749	6,873.7
J.P. Morgan Asset Management, Inc.	0.629	5,778.0
UBS Asset Management	0.603	5,536.3
Jennison Associates LLC	0.557	5,109.8
Morgan Stanley, Investment Banking and Brokerage Investments	0.522	4,788.1
Columbia Management Investment Advisers, LLC	0.459	4,214.1
Wellington Management Group LLP	0.441	4,051.3

Source: S&P Capital IQ

Annex 3. Relationships of Interest, Palantir and Amazon



Source: Empower LLC image, data from diverse government and corporate documents, websites.