From:	Brian Sterling (b)(6)
To:	Sterling, Brian (b)(6) (b)(6)
Subject:	Federal Agencies Use Cellphone Location Data for Immigration Enforcement - WSJ
Date:	2020/02/07 13:00:04
Priority:	Normal
Type:	Note

Federal Agencies Use Cellphone Location Data for Immigration Enforcement - WSJ

https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600

Sender:	Brian Sterling (b)(6)
Recipient:	Sterling, Brian (b)(6) (b)(6)
Sent Date:	2020/02/07 12:59:46
Delivered Date:	2020/02/07 13:00:04

From:	(b)(6)
To:	Quinn, Cameron (b)(6) (b)(6) Miller, Bennett (b)(6) (b)(6) Mina, Peter (b)(6) (b)(6) Sterling, Brian (b)(6) (b)(6) O'Malley, Ciaran (b)(6)
CC:	(b)(6)
Subject:	Article
Date:	2020/03/06 07:58:20
Priority:	Normal
Type:	Note

Interesting story on Federal (including DHS) law enforcement investigative use of contractor-collected mobile phone location data.

---

https://www.protocol.com/government-buying-location-data?xrs=RebelMouse_fb&ts=1583409914

Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones

Federal agencies have big contracts with Virginia-based Babel Street. Depending on where you've traveled, your movements may be in the company's data.

Charles Levinson
March 5, 2020

U.S. law enforcement agencies signed millions of dollars worth of contracts with a Virginia company after it rolled out a powerful tool that uses data from popular mobile apps to track the movement of people's cell phones, according to federal contracting records and six people familiar with the software.

The product, called Locate X and sold by Babel Street, allows investigators to draw a digital fence around an address or area, pinpoint mobile devices that were within that area, and see where else those devices have traveled, going back months, the sources told Protocol.

They said the tool tracks the location of devices anonymously, using data that popular cell phone apps collect to enable features like mapping or targeted ads, or simply to sell it on to data brokers.

Babel Street has kept Locate X a secret, not mentioning it in public-facing marketing materials and stipulating in federal contracts that even the existence of the data is "confidential information." Locate X must be "used for internal research purposes only," according to terms of use distributed to agencies, and law enforcement authorities are forbidden from using the technology as evidence — or mentioning it at all — in legal proceedings.

Federal records show that U.S. Customs and Border Protection purchased Locate X, and the Secret Service and U.S. Immigration and Customs Enforcement also use the location-tracking technology, according to a former Babel Street employee. Numerous other government agencies have active contracts with Reston-based Babel Street, records show, but publicly available contract information does not specify whether other agencies besides CBP bought Locate X or other products and services offered by the company.

None of the federal agencies, including CBP, would confirm whether they used the location-tracking software when contacted by Protocol. Babel Street's other products include an analytics tool it has widely marketed that sifts through streams of social media to "chart sentiment" about topics and brands.

A former government official familiar with Locate X provided an example of how it could be used, referring to the aftermath of a car bombing or kidnapping. Investigators could draw what is known as a geo-fence around the site, identify mobile devices that were in the vicinity in the days before the attack, and see where else those devices had traveled in the days, weeks or months leading up to the attack, or where they traveled afterward.

"If you see a device that a month ago was in Saudi Arabia, then you know maybe Saudis were involved," this person said. "It's a lead generator. You get a data point, and from there you use your other resources to figure out if it's valid."

A former Babel Street employee said the technology was deployed in a crackdown on credit card skimming, in which thieves install illegal card readers on gas station pumps, capturing customers' card data to use or sell online. The Secret Service was the lead agency in those investigations, which, according to published reports, led to arrests and the seizure of devices.

A spokesperson for the Secret Service declined to comment on its work with Babel Street, saying the agency does not reveal methods used to carry out missions.

While federal records show that CBP purchased Locate X and last year upgraded, paying for "premium" licenses, the records neither describe what Locate X does nor define the difference between a basic and premium license. A CBP spokesperson would not comment in detail about the use of the tool, but said the agency follows the law when deploying "open-source information."

Told of Protocol's reporting on Babel Street, Sen. Ron Wyden, a Democrat from Oregon who has pushed for tougher privacy legislation, questioned whether uses of the technology might violate the Fourth Amendment ban on unreasonable searches.

The Supreme Court, in the landmark case Carpenter v. United States, ruled in June 2018 that the government must obtain a search warrant to access cell-tower location data for individual phone accounts. The court "recognized that the government needs a warrant to get someone's location data," Wyden said. "Now the government is using its checkbook to try to get around Carpenter. Americans won't stand for that kind of loophole when it comes to our Fourth Amendment rights."

A spokesperson for Babel Street, Lacy Talton, declined to answer specific questions about the company's government sales or its Locate X technology, but said the firm handles data carefully

to comply with both the law and internet terms of service. There is no indication Babel Street is doing anything illegal.

"Although data content is freely available without restriction from thousands of vendors and suppliers, Babel Street employs a variety of measures to ensure appropriate use of the data," Talton said in a statement to Protocol. "This is not required by most vendors but stems from Babel Street's ethos of proper data compliance. The company regularly ensures that the data accessed through its software is in compliance with ever-changing global privacy regulations, data use rights, and terms of service."

The details of Babel Street's location-tracking technology and its contracts with the federal government have not been reported before. Last month, The Wall Street Journal reported that border and immigration agents were tracking the location of cell phones, and looking for activity in suspicious places near the border, after buying data from Venntel Inc. of Herndon, Virginia. Venntell is a subsidiary of location-based marketing company Gravy Analytics of Dulles, Virginia. Gravy Analytics has provided location data to Babel Street, according to former employees of both firms.

Taken together, the revelations suggest that the sale of personal location data from commercial firms to the government is more widespread and has been going on longer than previously known. The emergence of the technology comes amid growing, broader concern over the tracking of people's movements, whether through facial recognition, their license plates or the phones in their pockets.

While consumers enable location-based services on their cell phone apps, privacy advocates said people are generally unaware of how far their personal information could travel — and in particular that it could be piped to law enforcement.

The sources who spoke to Protocol, who independently described the location-tracking technology, were three former Babel Street employees, a former government official with firsthand knowledge of the company's products, and two former employees of Gravy Analytics. They requested anonymity because the information is sensitive, and some feared retribution from employers for speaking to the media.

A spokesperson for Gravy Analytics declined to comment on the company's relationship with Babel Street. She said Venntel is a "wholly owned subsidiary of Gravy Analytics that supports public sector initiatives."

She pointed to the company's privacy policy on its Web site: "We take consumer privacy seriously and ensure that our data platform remains fully transparent and compliant with industry and legal requirements," the policy reads. "Gravy ensures that 100% of our data complies with all local privacy laws, including required consumer consent and opt-out provisions."

From brand to threat management

While there is little public information about Locate X, government contracting records provide a picture of Babel Street's growth and increasing popularity in federal law enforcement circles. The company registered Locate X with the U.S. Patent and Trademark Office in May 2017, and sales to federal agencies shot up afterward — from $64,000 in fresh contracts in 2016 to more than $2.1 million in 2017 to nearly $5.3 million in 2018.

Babel Street's sales spike was fueled in large part by four new customers: CBP, which signed $3.2 million in contracts, ICE ($1.1 million), the State Department's Bureau of Diplomatic Security ($710,000), and the Secret Service's Criminal Investigations Division ($313,858), the records show.

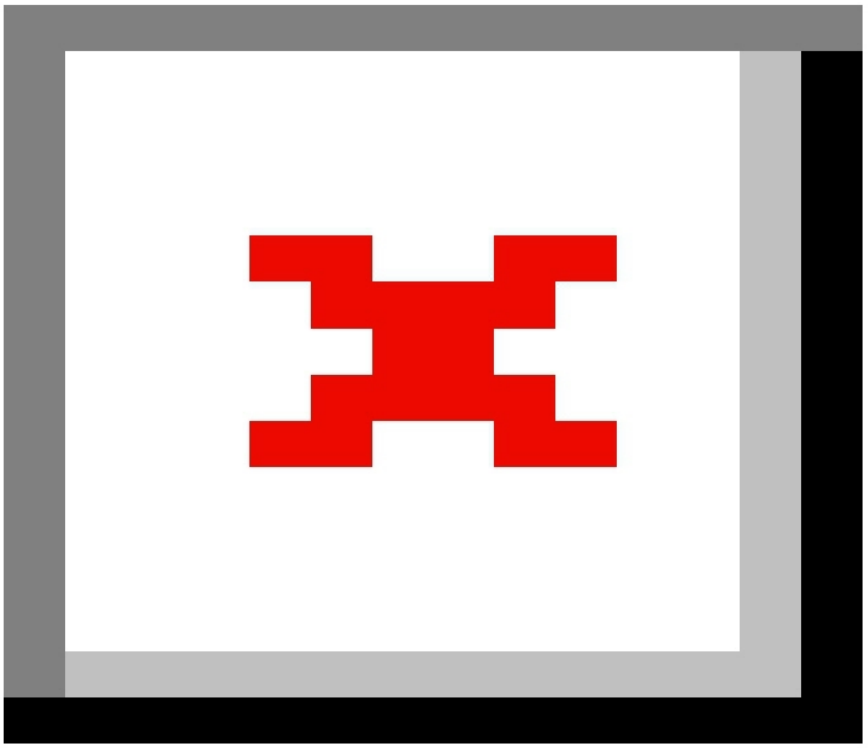
CBP signed a first contract worth $981,000 for "Babel software" in September 2017. The Targeting and Analysis Systems Directorate, the CBP branch that purchased the software, apparently liked what it received. A year later, the agency signed a fresh contract worth $2.2 million for "Babel software licenses." In March 2019, CBP filed an amended contract, worth an

extra $130,000, to "upgrade the current Babel Street Locate X licensing from basic to premium licenses as well as add an additional 10 licenses."
Asked about its use of Locate X, a CBP spokesperson told Protocol the agency uses a "variety of tools" that "may include tools to facilitate access to open-source data relevant to its border security mission. All CBP operations in which open-source information may be used are undertaken in furtherance of CBP's responsibility to enforce U.S. law at the border and in accordance with relevant legal, policy and privacy requirements."
In September 2018, ICE officials signed a one-year, $1.1 million contract with Babel Street. The deal included Locate X, according to a former Babel Street employee. Last August, ICE signed a fresh five-year deal worth up to $6.5 million with Babel Street for "data subscription services," records show.
A spokesperson for ICE said, "We do not discuss specific law enforcement tactics or techniques, or discuss the existence or absence of specific law-enforcement-sensitive capabilities." She also said, referring to cell phone location data, "ICE does not generally use this type of information for routine enforcement operations."
Other agencies with active Babel Street contracts include the Department of Justice, the U.S. Marshals Service, the Army, the Coast Guard, the Drug Enforcement Administration and the Department of Transportation's Office of Intelligence, Security and Emergency Response. The contract records are from USAspending.gov, the official source for U.S. government spending.
A spokesperson for the Department of Transportation, which signed a yearlong contract with Babel Street last May, said the Office of Intelligence, Security and Emergency Response "utilizes Babel Street software features depending on the nature of particular incidents."
Spokespeople for the Army, the Bureau of Diplomatic Security, the DEA and the Marshals Service declined to comment on the contracts with Babel Street. The Department of Justice and the Coast Guard did not respond to requests for comment.
A spokesperson for a regional DEA office in El Paso, Texas, which signed a separate $12,978 contract for a one-year Babel Street software license last September, denied that the agency had purchased the location-tracking data tool.
The technology was controversial enough that some agencies, including the FBI and the ATF, declined to purchase Locate X after those agencies' lawyers nixed it, a former Babel Street employee said.
A spokesperson for the FBI declined to comment. A spokesperson for the ATF, April Langwell, declined to comment on ATF procurement decisions. "ATF always works within DOJ guidelines with regard to the investigative techniques that we use and ensure that they are consistent with federal law and subject to court approval," Langwell said.
The former Babel Street employees and the former government official said Babel Street was careful about its clients for location data technology. For example, they said, it did not sell to commercial clients, local law enforcement agencies or foreign governments.
The software included pop-ups that reminded users it was to be used only in the investigation of serious crimes and matters of national security, one former employee said. However, after users complained that the pop-ups were annoying, the company removed them, the employee said. Babel Street did not respond to emailed questions about the pop-ups.

Secrecy to the extreme

Despite the apparent power of the tool, Protocol could not find a single instance in which a federal agency had publicly described using Locate X, in an investigation or in any other capacity. And Babel Street appears to have taken a number of steps to keep the technology secret. The company advertises other products on its website and in press releases, but makes no mention of Locate X or the tracking of mobile devices.
Locate X's terms of use, spelled out in a single document published online by the General Services Administration, require government clients to agree that the product "will be used for internal research purposes only. Locate X data may not be used as the basis for any legal

process in any country, including as the basis for a warrant or subpoena, or any other legal or administrative action." The terms state that Locate X data may not be "cited in any court/investigation-related document."



Tear-out

-
-

Terms of use for Babel Street's Locate X product state that the data "may not be used as the basis for any legal process."Illustration: 615 Productions

Protocol shared the terms of use in the Locate X contract with Nathan Wessler, a lawyer with the ACLU's Speech, Privacy, and Technology Project who argued the Carpenter v. United States case before the Supreme Court. He called the secrecy provisions "tremendously disturbing," raising the possibility that a criminal defendant might not know the tool had factored into a case — and therefore wouldn't be able to challenge its legality.

"These secrecy provisions prevent the courts from providing oversight," Wessler said. "That is really corrosive to our system of checks and balances."

In the past, Wessler noted, courts have been critical of nondisclosure agreements with law enforcement that are designed to protect sensitive surveillance technologies, notably in cases involving devices that mimic cell towers in order to capture phone information, often referred to by the brand name StingRays.

Scores of U.S. law enforcement agencies deployed the devices for years in secret without judicial scrutiny or public transparency. When use of the technology began to be exposed in criminal trials, the courts did not take a favorable view of the secrecy agreements. One of the more pointed opinions came in a 2016 ruling by a Maryland state appeals court judge, involving Baltimore police and an attempted murder suspect.

The use of a nondisclosure agreement to protect the technology is "inimical to the constitutional principles we revere," Judge Andrea M. Leahy wrote for the three-member court panel.

In 2015, both the Department of Justice and Homeland Security updated their policies to require law enforcement to disclose the use of cell site simulator technologies to the courts when used as part of an investigation. "In all circumstances, candor to the court is of paramount importance," the Homeland Security policy reads. "Applications for the use of a cell site simulator must include sufficient information to ensure that the courts are aware that the technology may be used."

The limits of anonymity

One of the former Babel Street employees who spoke to Protocol cited another example of how Locate X could be used to protect U.S. national security. Investigators, this person said, could identify mobile devices carried near popular border crossing points into the U.S. and pull up the historical location data for those devices, viewing where they've been in the preceding months.

"If you are thinking about attack planning, and you know these devices were just at a Hezbollah or ISIS training camp, and now they're sitting in Juarez, maybe that matters," the former employee said.

Still, privacy experts told of Protocol's reporting on Locate X asserted that law enforcement officials' practice of buying data they would otherwise need a warrant to access amounts to a form of data laundering.

"That consumers can have data being collected that tracks their location, and the government, instead of getting a warrant, which they would normally need to do, can just go to a private company and buy it directly, that's hugely concerning," said Serge Egelman, a computer science professor at UC Berkeley who works on privacy issues.

In the Supreme Court's Carpenter v. United States case, the court held that investigators violated the Fourth Amendment by obtaining cell tower records without a warrant that placed a robbery suspect near the crimes. Chief Justice John Roberts wrote, in the majority opinion, that authorities in that case had failed "to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years."

But whether courts would hold anonymous location data culled from mobile apps to the same standard is an open question.

A spokesperson for Wyden said the senator's aides had a phone call with Venntel attorneys on Feb. 20, in response to The Wall Street Journal article, to discuss the company's sale of location

data to the government. A Wyden aide said Venntel's counsel declined to answer most questions, would not identify the company's government clients, and would not reveal the source of the data.

Babel Street's sale of location data to the government could also raise potential liability issues for app developers under the Stored Communications Act, said Wessler, the ACLU lawyer. The 1986 law prohibits providers of computing services or electronic communication to the public from knowingly divulging customer information to any government entity.

"The question for the app companies themselves is whether, now that they know that Babel Street is taking their customers' location data and providing it to law enforcement, are those companies themselves now liable under the Stored Communications Act," Wessler said.

Location data culled from mobile apps is said to be anonymized, with each device masked behind a nameless ID number. But experts say data can be traced back to individual users, based on their particular movements.

The New York Times reviewed a database of location data and reported in December 2018 that it was able to identify a woman as she traveled to her dermatologist's office, hiked with her dog and stayed over at her ex-boyfriend's home. Babel Street did not respond to an emailed question about whether Locate X data can be de-anonymized.

Big sales, big hires

Babel Street was founded in 2009 as Agincourt Solutions by former U.S. Navy Officer Jeff Chapman, and became Babel Street in 2014. On its website and in marketing materials, it describes itself as "the world's data-to-knowledge company," focusing on a service that analyzes streams of social media activity in multiple languages, often for brand management and sometimes linked to locations such as sports arenas.

Early on, the promise of gleaning meaningful intelligence from Twitter feeds and other social media applications drew clients to Babel Street, according to government records, published reports and the former employees. The NFL has used Babel Street's analytics software. So, too, have at least 10 local law enforcement agencies around the country, according to the Brennan Center for Justice at New York University Law School.

Motherboard and The Washington Post wrote about the company's social media analytics software in 2017, noting heavy interest from police agencies overseeing major events like Super Bowls. On the government side, the FBI and the Army were among Babel Street's early customers. Michael Flynn, who served briefly as President Trump's national security adviser and later pleaded guilty to lying to the FBI, was once an adviser to the firm, according to Flynn's financial disclosure forms.

Just before the rollout of Locate X, the company hired a veteran Department of Justice privacy lawyer, Jill Maze, to be the company's chief privacy officer, according to former employees and Maze's LinkedIn account.

Subsequent hires suggest the company viewed location data as a growth area. In February 2019, Babel Street hired retired Maj. Gen. Mark Quantock, a former director of intelligence for U.S. Central Command, which includes the Middle East and Central Asia, and the former director of operations for the National Geospatial Intelligence Agency, essentially the government's headquarters for location data intelligence.

Three months later, the company hired a 20-year Pentagon veteran, Dave Dillow, who since 2003 has worked with special operations forces focused on integrating "publicly available information," or PAI, into the intelligence pipeline for those forces. Commercial location data is one type of PAI.

Get in touch with us: Share information securely with Protocol via encrypted Signal or WhatsApp message, at 415-214-4715 or through our anonymous SecureDrop.

The data used by Babel Street, said the former employees of Babel Street and Gravy Analytics, comes largely from third-party data aggregators who broker deals with mobile app developers, offering revenue in return and sometimes detailed analysis about how users are engaging with

the app. Data aggregators who spoke to Protocol said they enable services like mapping and marketing, and comply with privacy regulations, which include requiring all app users to give their consent to sharing their data.
Privacy advocates say such consumer opt-ins are often buried in small print or otherwise clouded in vague or bureaucratic language, and that users have little visibility into how their data is used.
"That's the fundamental problem," said Egelman, the UC Berkeley professor. "The trafficking in this data is totally opaque to everyone who isn't a party to these transactions."

Charles Levinson
Charles Levinson (@levinsonc) is a senior reporter at Protocol. Previously, he worked on investigative projects at Reuters, where he won awards for his reporting on Guantanamo Bay and skullduggery on Wall Street. Before that, he spent 12 years as a foreign correspondent in the Middle East for The Wall Street Journal. He covered the U.S. occupation of Iraq and that country's sectarian civil war, the Arab Spring uprisings in Tunisia, Egypt, Libya, Bahrain, and Syria, and Israel's wars in Lebanon and Gaza. He has reported from over 20 countries. He lives outside New York City.

V/r,

(b)(6)

(b)(6)
Senior Policy Advisor
DHS Office for Civil Rights
and Civil Liberties
(b)(6)
(b)(6)
Notify me via UNCLAS email or call
priot to Initiating a secure discussion.

Sender:	(b)(6)
Recipient:	Quinn, Cameron (b)(6) (b)(6) Miller, Bennett (b)(6) (b)(6) Mina, Peter (b)(6) (b)(6) Sterling, Brian (b)(6) (b)(6) (b)(6)

	(b)(6)
Sent Date:	2020/03/06 07:58:19
Delivered Date:	2020/03/06 07:58:20

From:	Sterling, Brian (b)(6)
	(b)(6)
To:	
Subject:	QFR FYI
Date:	2020/07/10 16:44:04
Priority:	Normal
Type:	Note

Sharing FYSA. Questions and responses on biometrics, cell location data, trusted traveler are good to know.

I cleared the tasker associated with this. Nothing for you to do.

Brian Sterling
Section Chief
Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
(b)(6) (desk)
(mobile)

Sender:	Sterling, Brian (b)(6)
	(b)(6)
Recipient:	
Sent Date:	2020/07/10 16:43:34
Delivered Date:	2020/07/10 16:44:04

From:	Sterling, Brian (b)(6)
To:	(b)(6)
Subject:	RE: ICE DRAFT FOR CLEARANCE - AS1 Correspondence re: reports that DHS purchased data and software that tracks the location for immigration enforcement purposes (WF #1191089)
Date:	2020/08/10 16:36:38
Priority:	Normal
Type:	Note

Thanks for this, (b)(6) I'm going to pass this along for tasker clearance.

Would you please mention this topic the next time you speak with (b)(6); (or someone else) at ICE?

(b)(5)

Brian Sterling
DHS CRCL
(b)(6) (desk)
(mobile)

From: (b)(6)
Sent: Monday, August 10, 2020 4:28 PM
To: Sterling, Brian (b)(6)
Subject: RE: ICE DRAFT FOR CLEARANCE - AS1 Correspondence re: reports that DHS purchased data and software that tracks the location for immigration enforcement purposes (WF #1191089)

SIIP has reviewed a draft response to a letter sent to AS1 by Senator Markey on DHS' use of commercial software that tracks geo-locational data. (b)(5)
(b)(5)

(b)(5)

(b)(5)

(b)(6)
DHS CRCL
(b)(6)

From: Sterling, Brian (b)(6)
Sent: Monday, August 10, 2020 10:46 AM
To: (b)(6)
Subject: FW: ICE DRAFT FOR CLEARANCE - AS1 Correspondence re: reports that DHS purchased data and software that tracks the location for immigration enforcement purposes (WF #1191089)

Hi (b)(6)

Would you please review this today.

Thanks,
Brian

Brian Sterling
DHS CRCL
(b)(6) (desk)
(mobile)

From: CRCL Exec Sec <(b)(6)
Sent: Monday, August 10, 2020 10:17 AM
To: Dallam, Elizabeth (b)(6)
(b)(6) Sterling, Brian
(b)(6)
Cc: Venture, Veronica (b)(6) Mina, Peter (b)(6)
Salvano-Dunn, Dana (b)(6) PORTO, VICTORIA
(b)(6) CRCL Exec Sec
(b)(6) Amendolia, Deana (b)(6)
Subject: Task Status Report: ICE DRAFT FOR CLEARANCE - AS1 Correspondence re: reports that DHS purchased data and software that tracks the location for immigration enforcement purposes (WF #1191089)

Good morning, SIIP/I-section:
Sorry this draft was inadvertently not circulated. It was originally tasked in February. Please see the attached and advise if there are comments.

<< File: Markey Draft Enclosure - 08.03.2020.docx >> << File: Markey Draft Cover Letter - 08.03.2020.docx >>

-----Original Message-----
From: (b)(6)
Sent: Monday, August 10, 2020 7:44 AM
To: CRCL Exec Sec (b)(6)
Subject: Clearance Status Requested. (Service 1191089) (Intranet Quorum IMA007540485)

CRCL / PRIV:

Regarding WF 1191089 – please provide a status update.

Thank you for your time, consideration, and help with this request.

Best,

(b)(6)
Correspondence Specialist
Office of the Executive Secretariat
Office of the Director
U.S. Immigration and Customs Enforcement
(b)(6) (o)
(c)
(b)(6)

Contact: The Honorable Edward J. Markey

https://IQ.dhs.gov/iq/UX/serviceitem.aspx?id=1191089&iAccount=IQ

Sincerely,

(b)(6)
DHS/CRCL/CRCL ExecSec
(b)(6) office
mobile

-----Original Task-----
Subject: ICE DRAFT FOR CLEARANCE TO COME - AS1 Correspondence re: reports that DHS purchased data and software that tracks the location for immigration enforcement purposes (WF #1191089)
Priority: Normal
Due date: Thu 2/20/2020

Status: Not Started
% Complete: 0%
Actual work: 0 hours

Requested by: CRCL Exec Sec

Lead: SIIP
~~Coord.: I-section~~
Cc: Ronnie, Peter, Dana, Becky, (b)(6)

ICE draft to be circulated at a later date for CRCL comment/clearance.

<< File: WF1191089 incoming.pdf >>

~(b)(6)

-----Original Message-----
From: CRCL Exec Sec
Sent: Thursday, February 13, 2020 11:30 AM
To: Sterling, Brian (b)(6); Dallam, Elizabeth (b)(6)
(b)(6)
(b)(6); Venture, Veronica (b)(6) Mina, Peter
(b)(6) Salvano-Dunn, Dana (b)(6) Tosado, Rebekah
(b)(6)
Cc: CRCL Exec Sec (b)(6) Amendolia, Deana (b)(6)
Subject: AS1 Correspondence re: reports that DHS purchased data and software that tracks the location of individuals and is using this for immigration enforcement purposes.Clearing Component (WF #1191089)

SIIP/I-section: tasker to be sent. Please let me know if others should be included.

Sincerely,

(b)(6)
DHS/CRCL/CRCL ExecSec
(b)(6) office
mobile

-----Original Message-----
From (b)(6)
Sent: Thursday, February 13, 2020 9:53 AM
To: CRCL Exec Sec (b)(6)
Subject: Clearing Component (Service 1191089) (Intranet Quorum IMA007360444)

MGMT / OLA / OGC / CBP / PRIV / CRCL: ICE has the lead to prepare a draft in response to the attached incoming. Please share this incoming with your leadership. If your leadership has any comments,

concerns, or issues that should be incorporated into the draft response, please share them with the drafting component within 24 hours so that the issues can be addressed prior to submitting the draft to ESEC

Contact: The Honorable Edward J. Markey

https://IQ.dhs.gov/iq/UX/serviceitem.aspx?id=1191089&iAccount=IQ

Sender:	Sterling, Brian (b)(6)
Recipient:	(b)(6)
Sent Date:	2020/08/10 16:36:37
Delivered Date:	2020/08/10 16:36:38

From:	(b)(6)
To:	Sterling, Brian (b)(6) (b)(6)
Subject:	FW: Senators Urge Investigation After CBP Admits to Warrantless Cell Phone Surveillance - Nextgov - Compliance seeking SIIP's perspective, please
Date:	2020/10/29 15:52:59
Due Date:	2020/10/28 20:00:00
Priority:	Normal
Type:	Note

Hi, (b)(6)

I know you have many competing priorities. I wanted to let you know that we didn't have time for me to present these two articles about CBP contracting with a data broker and not providing Congress legal analysis this morning at our case opening meeting.

https://urldefense.us/v3/__https://www.vice.com/en/article/n7vwex/cbp-dhs-venntel-location-data-no-warrant__;!!BClRuOV5cvtbuNI!QgqlxeApVZZ7X25Twz3lEiwllZ2RwUNc9VC4DnSdBUUSnISLn_vgIGGGAhVS4MH6pqVjmnk5tRwe$

https://urldefense.us/v3/__https://www.nextgov.com/analytics-data/2020/10/senators-urge-investigation-after-cpb-admits-warrantless-cell-phone-surveillance/169562/__;!!BClRuOV5cvtbuNI!RzcNKDASjU9coXlg6Sg2mcmWxduY1Ux7cMsJb7_qK43hmdlulWxHAxTohFuUz9Gpn1xWKGvSu28$

I'm meeting with Dana tomorrow, Friday, October 30 at 2PM in case you had the time to take a quick look at these articles and offer any preliminary thoughts from SIIP's perspective before then, please.

Thank you for your consideration.

Best,

(b)(6)

(b)(6)
Senior Policy Advisor, Compliance Branch
DHS, Office for Civil Rights and Civil Liberties

(b)(6) - Mobile
(b)(6)

From: (b)(6)
Sent: Wednesday, October 28, 2020 10:03 AM
To: Sterling, Brian (b)(6)
Subject: FW: Senators Urge Investigation After CBP Admits to Warrantless Cell Phone Surveillance - Nextgov

Good morning, Brian.

Compliance is processing two articles covering the same subject, CBP using subscriptions with a data broker Venntel, a government contractor, which gives CBP access to commercial location data and CBP will not provide its legal analysis to Congress. One article is below and the other id farther down in this chain. Dana asked me to check with SIIP. Thanks for any thoughts you may have. I'm hoping to process them and bring them to our case opening tomorrow morning, if you have any initial thoughts later today. Thanks, Brian.

https://urldefense.us/v3/__https://www.vice.com/en/article/n7vwex/cbp-dhs-venntel-location-data-no-warrant__;!!BClRuOV5cvtbuNI!QgqlxeApVZZ7X25Twz3lEiwllZ2RwUNc9VC4DnSdBUUSnISLn_vgIGGGAhVS4MH6pqVjmnk5tRwe$

(b)(6)

(b)(6)
Senior Policy Advisor, Compliance Branch
DHS, Office for Civil Rights and Civil Liberties
(b)(6) - Mobile
(b)(6)

This message may contain information that is confidential, deliberative, law enforcement sensitive, and/or otherwise protected from public disclosure. If it has been sent to you in error, please reply immediately to advise the sender of the error and then destroy this message, any copies of this message and any printout of this message. If you are not the intended recipient of the message, any unauthorized dissemination, distribution or copying of the material in this message, and any attachments to the message, is strictly forbidden. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. §§ 552(b)(5), (b)(6), and/or (b)(7).

From: Salvano-Dunn, Dana (b)(6)
Sent: Wednesday, October 28, 2020 9:21 AM
To: (b)(6) CRCLCompliance <CRCLCompliance@HQ.DHS.GOV>
Cc: McKenney, William (b)(6)
(b)(6)
Subject: RE: Senators Urge Investigation After CBP Admits to Warrantless Cell Phone Surveillance - Nextgov

Thanks (b)(6) !

From: (b)(6)
Sent: Wednesday, October 28, 2020 9:01 AM
To: Salvano-Dunn, Dana (b)(6) CRCLCompliance <CRCLCompliance@HQ.DHS.GOV>
Cc: McKenney, William (b)(6)
(b)(6)
Subject: RE: Senators Urge Investigation After CBP Admits to Warrantless Cell Phone Surveillance - Nextgov

ok

(b)(6)

(b)(6)
Senior Policy Advisor, Compliance Branch
DHS, Office for Civil Rights and Civil Liberties
(b)(6) - Mobile
(b)(6)

This message may contain information that is confidential, deliberative, law enforcement sensitive, and/or otherwise protected from public disclosure. If it has been sent to you in error, please reply immediately to advise the sender of the error and then destroy this message, any copies of this message and any printout of this message. If you are not the intended recipient of the message, any unauthorized dissemination, distribution or copying of the material in this message, and any attachments to the message, is strictly forbidden. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. §§ 552(b)(5), (b)(6), and/or (b)(7).

From: Salvano-Dunn, Dana (b)(6)
Sent: Wednesday, October 28, 2020 7:55 AM
To: CRCLCompliance <CRCLCompliance@HQ.DHS.GOV>
Cc: (b)(6) McKenney, William
(b)(6)
Subject: Fwd: Senators Urge Investigation After CBP Admits to Warrantless Cell Phone Surveillance - Nextgov

Pls have (b)(6) process. Pls also check in with SIIP re their thoughts.

From: Dana Salvano-Dunn (b)(6)
Sent: Wednesday, October 28, 2020 7:52 AM
To: Salvano-Dunn, Dana
Subject: Senators Urge Investigation After CBP Admits to Warrantless Cell Phone Surveillance - Nextgov

https://urldefense.us/v3/__https://www.nextgov.com/analytics-data/2020/10/senators-urge-investigation-after-cpb-admits-warrantless-cell-phone-surveillance/169562/__;!!BClRuOV5cvtbuNI!RzcNKDASjU9coXlg6Sg2mcmWxduY1Ux7cMsJb7_qK43hmdlulWxHAxTohFuUz9Gpn1xWKGvSu28$

Sent from my iPhone

Sender:	(b)(6)
Recipient:	Sterling, Brian (b)(6) (b)(6)
Sent Date:	2020/10/29 15:52:58
Delivered Date:	2020/10/29 15:52:59

From:	(b)(6)
To:	Sterling, Brian (b)(6)
CC:	(b)(6)
Subject:	RE: Contact-DHS-21-0254 and Contact-DHS-21-0243 related to CBP and Venntel contract
Date:	2020/10/30 16:12:53
Priority:	Normal
Type:	Note

Excellent! Thank you, Brian and (b)(6)

Best,

(b)(6)

(b)(6)
Senior Policy Advisor, Compliance Branch
DHS, Office for Civil Rights and Civil Liberties
(b)(6) - Mobile
(b)(6)

From: Sterling, Brian (b)(6)
Sent: Friday, October 30, 2020 4:01 PM
To: (b)(6)
Cc:
Subject: RE: Contact-DHS-21-0254 and Contact-DHS-21-0243 related to CBP and Venntel contract

Thanks, (b)(6) SIIP would be happy to participate. I'm asking (b)(6) to take up this issue for us. He'll review the questions and get back to you next week.

Have a nice weekend!

Thanks,

Brian

Brian Sterling
DHS CRCL
(b)(6) (desk)
(mobile)

From: (b)(6)
Sent: Friday, October 30, 2020 3:57 PM
To: Sterling, Brian (b)(6)
Subject: Contact-DHS-21-0254 and Contact-DHS-21-0243 related to CBP and Venntel contract

Dear Brian,

Thanks again for our call earlier today.

At the meeting with Dana, Bill, Deborah, and others on the two above-referenced contacts this afternoon, Dana directed me to request a briefing from CBP prior to her making a decision whether to open a complaint. Compliance would like SIIP to participate in the briefing as well, please.

To that end, I have drafted several questions to send to CBP on the scope of the briefing based on the two articles below:

https://urldefense.us/v3/__https://www.vice.com/en/article/n7vwex/cbp-dhs-venntel-location-data-no-warrant__;!!BClRuOV5cvtbuNI!QgqlxeApVZZ7X25Twz3lEiwIlZ2RwUNc9VC4DnSdBUUSnISLn_vgIGGGAhVS4MH6pqVjmnk5tRwe$

https://urldefense.us/v3/__https://www.nextgov.com/analytics-data/2020/10/senators-urge-investigation-after-cpb-admits-warrantless-cell-phone-surveillance/169562/__;!!BClRuOV5cvtbuNI!RzcNKDASjU9coXlg6Sg2mcmWxduY1Ux7cMsJb7_qK43hmdlulWxHAxTohFuUz9Gpn1xWKGvSu28$

I would appreciate your help by providing your input regarding these draft questions for the briefing, please:

1. (b)(5)

2. (b)(5)

3.

4.

5.

Thanks for your feedback on these questions and offering your ideas for other questions, Brian.

Best,

(b)(6)

(b)(6)

Senior Policy Advisor, Compliance Branch
DHS, Office for Civil Rights and Civil Liberties
(b)(6) - Mobile
(b)(6)

Sender:	(b)(6)
Recipient:	Sterling, Brian (b)(6) (b)(6)
Sent Date:	2020/10/30 16:12:53