

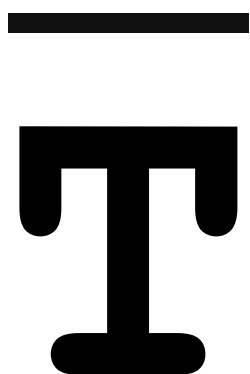
STINGRAYS

A Secret Catalogue of Government Gear for Spying on Your Cellphone



Jeremy Scahill, Margot Williams

Dec. 17 2015, 6:23 p.m.



HE INTERCEPT HAS OBTAINED

a secret, internal U.S. government [catalogue](#) of dozens of cellphone surveillance devices used by the military and by intelligence agencies. The document, thick with previously undisclosed information, also offers rare insight into the spying capabilities of federal law enforcement and local police inside the United States.

The catalogue includes details on the Stingray, a well-known brand of surveillance gear, as well as Boeing “dirt boxes” and dozens of more



68



be discreetly carried by an individual. They have names like Cyberhawk, Yellowstone, Blackfin, Maximus, Cyclone, and Spartacus. Within the catalogue, the NSA is listed as the vendor of one device, while another was developed for use by the CIA, and another was developed for a special forces requirement. Nearly a third of the entries focus on equipment that seems to have never been described in public before.



The Intercept obtained the catalogue from a source within the intelligence community concerned about the militarization of domestic law enforcement. (The original is [here](#).)

A few of the devices can house a “target list” of as many as 10,000 unique phone identifiers. Most can be used to geolocate people, but the documents indicate that some have more advanced capabilities, like eavesdropping on calls and spying on SMS messages. Two systems, apparently designed for use on captured phones, are touted as having the ability to extract media files, address books, and notes, and one can retrieve deleted text messages.

used by law enforcement agencies to spy on people and convict them of crimes. The mass shooting earlier this month in San Bernardino, California, which President Barack Obama has called “an act of terrorism,” prompted [calls](#) for state and local police forces to beef up their counterterrorism capabilities, a process that has historically involved adapting military technologies to civilian use. Meanwhile, civil liberties advocates and others are increasingly alarmed about how cellphone surveillance devices are used domestically and have called for a more open and informed debate about the trade-off between security and privacy — despite a virtual blackout by the federal government on any information about the specific capabilities of the gear.

“We’ve seen a trend in the years since 9/11 to bring sophisticated surveillance technologies that were originally designed for military use — like Stingrays or drones or biometrics — back home to the United States,” said Jennifer Lynch, a senior staff attorney at the Electronic Frontier Foundation, which has waged a legal battle challenging the use of cellphone surveillance devices domestically. “But using these technologies for domestic law enforcement purposes raises a host of issues that are different from a military context.”

M

ANY OF THE DEVICES in the catalogue, including the Stingrays and dirt boxes, are cell-site simulators, which operate by mimicking the towers of major telecom companies like Verizon, AT&T, and T-Mobile. When someone’s phone connects to the spoofed network, it transmits a unique identification code and, through the characteristics of its radio signals when they reach the receiver, information about the phone’s location. There are also [indications](#) that cell-site simulators may be able to monitor calls and text messages.

In the catalogue, each device is listed with guidelines about how its use



68



and intelligence operations, including covert action.

But domestically the devices have been used in a way that violates the constitutional rights of citizens, including the Fourth Amendment prohibition on illegal search and seizure, critics like Lynch say. They have regularly been used without warrants, or with warrants that critics call overly broad. Judges and civil liberties groups alike have complained that the devices are used without full disclosure of how they work, even within court proceedings.

“Every time police drive the streets with a Stingray, these dragnet devices can identify and locate dozens or hundreds of innocent bystanders’ phones,” said Nathan Wessler, a staff attorney with the Speech, Privacy, and Technology Project of the American Civil Liberties Union.

The controversy around cellphone surveillance illustrates the friction that comes with redeploying military combat gear into civilian life. The U.S. government has been using cell-site simulators for at least [20 years](#), but their use by local law enforcement is a more recent development.

The archetypical cell-site simulator, the Stingray, was trademarked by Harris Corp. in 2003 and initially used by the military, intelligence agencies, and federal law enforcement. Another company, Digital Receiver Technology, now owned by Boeing, developed dirt boxes — more powerful cell-site simulators — which gained favor among the NSA, CIA, and U.S. military as good tools for hunting down suspected terrorists. The devices can reportedly track more than 200 phones over a wider range than the Stingray.

Amid the war on terror, companies selling cell-site simulators to the federal government thrived. In addition to large corporations like Boeing and Harris, which clocked more than [\\$2.6 billion in federal contracts](#) last year, the catalogue obtained by *The Intercept* includes products from little-known outfits like Nevada-based Ventis, which appears to have been [dissolved](#), and SR Technologies of Davie, Florida, which has a website that warns:



68



by *The Intercept* is not dated, but includes information about an event that occurred in 2012.)

The U.S. government eventually used cell-site simulators to target people for assassination in drone strikes, *The Intercept* has [reported](#). But the CIA helped use the technology at home, too. For more than a decade, the agency worked with the U.S. Marshals Service to deploy planes with dirt boxes attached to track mobile phones across the U.S., the *Wall Street Journal* [revealed](#).

After being used by federal agencies for years, cellular surveillance devices began to make their way into the arsenals of a small number of local police agencies. By 2007, Harris sought a license from the Federal Communications Commission to widely sell its devices to local law enforcement, and police [flooded](#) the FCC with letters of support. “The text of every letter was the same. The only difference was the law enforcement logo at the top,” said Chris Soghoian, the principal technologist at the ACLU, who obtained copies of the letters from the FCC through a Freedom of Information Act request.

The lobbying campaign was a success. Today nearly 60 law enforcement agencies in 23 states are [known](#) to possess a Stingray or some form of cell-site simulator, though experts believe that number likely underrepresents the real total. In some jurisdictions, police use cell-site simulators regularly. The Baltimore Police Department, for example, has used Stingrays [more than](#) 4,300 times since 2007.

Police often cite the war on terror in acquiring such systems. Michigan State Police claimed their Stingrays would “allow the State to track the physical location of a suspected terrorist,” although the ACLU [later found](#) that in 128 uses of the devices last year, none were related to terrorism. In Tacoma, Washington, police [claimed](#) Stingrays could prevent attacks using improvised explosive devices — the roadside bombs that plagued soldiers in Iraq. “I am not aware of any case in which a police agency has used a cell-site simulator to find a terrorist,” said Lynch. Instead, “law enforcement

The Intercept is not publishing information on devices in the catalogue where the disclosure is not relevant to the debate over the extent of domestic surveillance.

The Office of the Director of National Intelligence declined to comment for this article. The FBI, NSA, and U.S. military did not offer any comment after acknowledging *The Intercept's* written requests. The Department of Justice “uses technology in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities,” said Marc Raimondi, a Justice Department spokesperson who, for six years prior to working for the DOJ, worked for Harris Corp., the manufacturer of the Stingray.

W

HILE INTEREST FROM local cops helped fuel the spread of cell-site simulators, funding from the federal government also played a role, incentivizing municipalities to buy more of the technology. In the years since 9/11, the U.S. has expanded its funding to provide military hardware to state and local law enforcement agencies via grants awarded by the Department of Homeland

Security and the Justice Department. There’s been a similar pattern with Stingray-like devices.

“The same grant programs that paid for local law enforcement agencies across the country to buy armored personnel carriers and drones have paid for Stingrays,” said Soghoian. “Like drones, license plate readers, and biometric scanners, the Stingrays are yet another surveillance technology created by defense contractors for the military, and after years of use in war zones, it eventually trickles down to local and state agencies, paid for with DOJ and DHS money.”



68



of Stingray devices [since 2008](#). In California, Alameda County and police departments in Oakland and Fremont [are using](#) \$180,000 in Homeland Security grant money to buy Harris' Hailstorm cell-site simulator and the hand-held Thoracic surveillance device, made by Maryland security and intelligence company Keyw. As part of Project Archangel, which is described in government contract documents as a "border radio intercept program," the Drug Enforcement Administration has contracted with Digital Receiver Technology for over \$1 million in DRT surveillance box equipment. The Department of the Interior contracted with Keyw for more than half a million dollars of "reduced signature cellular precision geolocation."

Information on such purchases, like so much about cell-site simulators, has trickled out through freedom of information requests and public records. The capabilities of the devices are kept under lock and key — a secrecy that harkens back to their military origins. When state or local police purchase the cell-site simulators, they [are routinely required](#) to sign non-disclosure agreements with the FBI that they may not reveal the "existence of and the capabilities provided by" the surveillance devices, or share "any information" about the equipment with the public.

Indeed, while several of the devices in the military catalogue obtained by *The Intercept* are actively deployed by federal and local law enforcement agencies, according to public records, judges have struggled to obtain details of how they work. Other products in the secret catalogue have never been publicly acknowledged and any use by state, local, and federal agencies inside the U.S. is, therefore, difficult to challenge.

"It can take decades for the public to learn what our police departments are doing, by which point constitutional violations may be widespread," Wessler said. "By showing what new surveillance capabilities are coming down the pike, these documents will help lawmakers, judges, and the public know what to look out for as police departments seek ever-more powerful electronic surveillance tools."

f

t



68



seized under federal civil forfeiture law, in drug busts and other operations. Illinois, Michigan, and Maryland police forces have all used asset forfeiture funds to pay for Stingray-type equipment.

“The full extent of the secrecy surrounding cell-site simulators is completely unjustified and unlawful,” said EFF’s Lynch. “No police officer or detective should be allowed to withhold information from a court or criminal defendant about how the officer conducted an investigation.”

J

JUDGES HAVE BEEN among the foremost advocates for ending the secrecy around cell-site simulators, including by pushing back on warrant requests. At times, police have attempted to hide their use of Stingrays in criminal cases, prompting at least one judge to throw out evidence obtained by the device. In 2012, a U.S. magistrate judge in Texas rejected an application by the Drug Enforcement

Administration to use a cell-site simulator in an operation, saying that the agency had failed to explain “what the government would do with” the data collected from innocent people.

Law enforcement has responded with some limited forms of transparency. In September, the Justice Department [issued](#) new guidelines for the use of Stingrays and similar devices, including that federal law enforcement agencies using them must obtain a warrant based on probable cause and must delete any data intercepted from individuals not under investigation.

Contained within the guidelines, however, is a clause stipulating vague “exceptional circumstances” under which agents could be exempt from the requirement to get a probable cause warrant.

“Cell-site simulator technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings,

f

t



68



Meanwhile, parallel [guidelines](#) issued by the Department of Homeland Security in October [do not require warrants](#) for operations on the U.S. border, nor do the warrant requirements apply to state and local officials who purchased their Stingrays through grants from the federal government, such as those in Wisconsin, Maryland, and Florida.

The ACLU, EFF, and several prominent members of Congress have said the federal government's exceptions are too broad and leave the door open for abuses.

“Because cell-site simulators can collect so much information from innocent people, a simple warrant for their use is not enough,” said Lynch, the EFF attorney. “Police officers should be required to limit their use of the device to a short and defined period of time. Officers also need to be clear in the probable cause affidavit supporting the warrant about the device’s capabilities.”

In November, a federal judge in Illinois published a legal memorandum about the government’s application to use a cell-tower spoofing technology in a drug-trafficking investigation. In his memo, Judge Iain Johnston sharply criticized the secrecy surrounding Stingrays and other surveillance devices, suggesting that it made weighing the constitutional implications of their use extremely difficult. “A cell-site simulator is simply too powerful of a device to be used and the information captured by it too vast to allow its use without specific authorization from a fully informed court,” [he wrote](#).

He added that Harris Corp. “is extremely protective about information regarding its device. In fact, Harris is so protective that it has been widely reported that prosecutors are negotiating plea deals far below what they could obtain so as to not disclose cell-site simulator information. ... So where is one, including a federal judge, able to learn about cell-site simulators? A judge can ask a requesting Assistant United States Attorney or a federal agent, but they are tight-lipped about the device, too.”

The ACLU and EFF believe that the public has a right to review the types of



68



Intercept, said Wessler, “fills an important gap in our knowledge, but it is incumbent on law enforcement agencies to proactively disclose information about what surveillance equipment they use and what steps they take to protect Fourth Amendment privacy rights.”

Research: Josh Begley

CONTACT THE AUTHOR:



Jeremy Scahill

✉ jeremy.scahill@theintercept.com

t [@jeremyscahill](https://twitter.com/jeremyscahill)



Margot Williams

✉ margot.williams@theintercept.com

t [@MargotWilliams](https://twitter.com/MargotWilliams)

V  68 Comments

THE DRONE PAPERS

secret documents detailing the inner workings of the U.S. military's assassination program in Afghanistan, Yemen, and Somalia. The documents, provided by a whistleblower, offer an unprecedented glimpse into Obama's drone wars.

[READ THE STORIES](#) →



THE ASSASSINATION COMPLEX

The whistleblower who leaked the drone papers believes the public is entitled to know how people are placed on kill lists and assassinated on orders from the president.



A VISUAL GLOSSARY

Decoding the language of covert warfare.



THE KILL CHAIN

New details about the secret criteria for drone strikes and how the White House approves targets.



68



CONGRESS JUST PUT IRANIAN-AMERICANS AND OTHERS AT RISK FOR BECOMING SECOND-CLASS CITIZENS

Murtaza Hussain

Dec. 18 2015, 10:27 p.m.



13



TODAY BOTH HOUSES OF CONGRESS approved a \$1.1 trillion spending bill intended to keep government services funded through September 2016. Tucked into this omnibus legislation are provisions that could undermine, on the basis of personal heritage, the ability of many

f

t



68



V

The new restrictions have alarmed civil rights groups in the United States, including the American Civil Liberties Union, which in a [letter](#) to the House

f

t



68



solely based on their nationality or ethnic origin. Despite this harsh criticism, at least some of the provisions were approved by the House of Representatives in a 407-19 vote on December 8, paving the way for today's vote.

Jamal Abdi, a spokesperson for the National Iranian American Council, believes the legislation will eventually prompt other countries to deny Iranian-Americans the same rights of free travel enjoyed by other Americans.

“Targeting people who are dual nationals is particularly discriminatory and unjust, since dual nationality is not something you choose,” Abdi said. “Under this legislation, if you're a European of Iranian origin or your father is an Iranian citizen, you wouldn't be able to travel without a visa to the United States. As we've already heard from the EU, this would trigger reciprocal measures that would result in the passports of Iranian-Americans being treated as inferior, essentially putting them in a category of second-class citizenship.”

The bill approved by the House earlier this month, [HR-158](#), which is related to the legislation approved today, was initially written for the narrow and reasonable purpose of blocking or restricting from U.S. entry individuals who traveled to Islamic State-controlled territory in Syria or Iraq. But provisions later added by Republican lawmakers made the legislation more draconian, including by imposing restrictions involving entire countries — official “state sponsors of terrorism” like Iran and Sudan. (In those two countries, at least, the Islamic State is nonexistent.)

Some parts of the newly passed legislation could even violate the recently negotiated deal between the U.S. and Iran to curb Iranian nuclear activity.

For example, under the new rules, a European or Japanese business owner who traveled to Iran to take advantage of recently lifted economic sanctions would thereafter find themselves denied visa-free entry to the



68



deal prohibit policies that undermine “the normalization of trade and economic relations with Iran.”

Thirty-three Democratic members of Congress signed an [open letter](#) published last week criticizing some of the new Visa Waiver Program restrictions. The letter said the restrictions “would result in discrimination against people simply because they are dual citizens based on ancestry” and asserted that national origin should not be a factor when determining visa requirements. People entering the United States, the letter said, should be evaluated on an individual level, not based on “where their parents are from.”

In the end, those objections were not enough to stop the new rules. Abdi said that politicians have stoked fears of immigration and helped increase public support for harsh laws that target en masse individuals from Muslim-majority countries.

“This bill is a direct response to the rhetoric of GOP leaders like Donald Trump and others who have called for restricting people coming to the United States based on national origin,” Abdi said. “There has been a lot of outcry about his outrageous comments and proposals from the public and in the media, but now as a consequence of the environment he’s helped create, we’re actually seeing Congress take steps to turn such xenophobic ideas into law.”

CONTACT THE AUTHOR:



Murtaza Hussain

murtaza.hussain@theintercept.com

[@mazmhussain](https://twitter.com/mazmhussain)



68



AL JAZEERA BLOCKS ANTI-SAUDI ARABIA ARTICLE

Cora Currier

Dec. 18 2015, 7:29 p.m.



7

america.aljazeera.com



This web page has a redirect
loop

ERR_TOO_MANY_REDIRECTS

THE CORPORATE HEADQUARTERS of Al Jazeera appears to have blocked an article critical of Saudi Arabia's human rights record from



Yemen kill civilians indiscriminately. The reports Sethi cites have been widely covered in the media ([including *The Intercept*.](#)) Sethi, who has



68



America had solicited the op-ed from him.

A few days after publication, Sethi's Twitter feed was flooded with attacks from pro-Saudi accounts. David Johnson, senior opinion editor at Al Jazeera America, [retweeted](#) many of the attacks. (He declined to be interviewed for this piece.)

"The trolling seemed like an organized concerted effort to intimidate me," Sethi said. "I will not submit to this act of censorship. Human rights are universal and I will continue to litigate and write about violations wherever they occur."

Qatar is a monarchy tightly ruled by the emir Sheikh Tamim bin Hamad al-Thani. The tiny, oil rich country has allied with Saudi Arabia against the government of Syria in that country's civil war, and is part of Saudi Arabia's campaign against the Houthi rebels in Yemen, contributing to the [devastating air war](#) and [deploying more](#) than 1,000 ground troops this fall. Qatar is also part of the 34-nation Islamic alliance against terrorism that Saudi Arabia [announced](#) this week.

The Saudi Arabian embassy in Washington, D.C., did not respond to questions about whether it had discussed the article with Al Jazeera or the Qatari government.

While Al Jazeera's international coverage has been praised — particularly in the years after the 9/11 attacks — this is not the first time that the network has appeared to [cater to the interests](#) of Qatar and its Gulf allies. (Disclosure: prior to joining *The Intercept*, I wrote an article for Al Jazeera America as a freelancer.)

It has been [criticized](#) for lack of coverage of protests against the government of Bahrain, for example, and in 2012, several journalists [complained](#) that they had to edit coverage of Syria to feature the emir of Qatar's position. In 2013, staffers in Egypt [resigned](#) in protest of the network's bias toward the Muslim Brotherhood after the military deposed the president, Mohamed Morsi. (The Egyptian government subsequently

f

t



68



freed in September.)

Al Jazeera America was founded in 2013 as the U.S. face of the network. It has struggled to gain a large audience and was roiled by [drama](#) this year, with the departure of several top executives amid allegations of sexism and workplace dysfunction. Qatar's emir also announced [cutbacks](#) in government support for the news network overall this year.

The apparent censorship of the Sethi article seems to be unprecedented, however. Several Al Jazeera America staffers said that they were unaware of another instance in which the parent company had blocked an article in this way.

CONTACT THE AUTHOR:



[Cora Currier](#)

[✉ cora.currier@theintercept.com](mailto:cora.currier@theintercept.com)

[t @coracurrier](#)



7 Comments

The
Intercept_

UNOFFICIAL
_SOURCES



68



Clinton, Rubio, Cruz Receive Foreign Policy Advice From Same Consulting Firm

Lee Fang

Dec. 18 2015, 6:46 p.m.



33

Consultants affiliated with a small Washington, D.C., firm called [Beacon Global Strategies](#) hold the unique privilege of providing high-profile foreign policy guidance to Hillary Clinton, Marco Rubio, and Ted Cruz, among others.

The bipartisan firm was founded in 2013 by former senior officials from the State Department, Department of Defense, and Central Intelligence Agency, and quickly had more than a dozen clients, primarily defense contractors, according to [Defense News](#).

f

t



68



V

Beacon Global Strategies [promoted](#) its influence over the 2016 presidential field on its website with an item [touting](#) Brian Hook's work to advise Republican candidates.



68



Washington as thousands of lobbyists have simply deregistered while continuing to peddle influence on behalf of clients. Under federal lobbying law, lobby registration is only required under very narrow guidelines that are [rarely enforced](#).

While Beacon Global Strategies' clients and services are a mystery, the firm maintains strong ties to Washington influencers. *Politico* Playbook [headlined](#) the launch of the group: "HOT NEW NATIONAL-SECURITY FIRM."

After the launch, Jeremy Bash, the managing director of the firm, joined the advisory board to Paladin Capital Group, a private equity firm that provides funding for start-ups that [serve](#) as contractors to the National Security Agency.

Beacon Global Strategies' seed funding came from Claude Fontheim, a former Clinton adviser who now serves as a [lobbyist](#) to the U.S.-China Exchange Foundation, a nonprofit [reportedly](#) used by Chinese government officials and Hong Kong tycoons to [shape](#) American policy toward China.

CONTACT THE AUTHOR:



Lee Fang

[✉ lee.fang@theintercept.com](mailto:lee.fang@theintercept.com)

[t @lhfang](#)

[intercept](#)
UNOFFICIAL
_SOURCES

Last-Minute Budget Bill Allows New Privacy-Invasive Surveillance in the Name of Cybersecurity

Jenna McLaughlin

Dec. 18 2015, 2:20 p.m.



In the wake of a series of humiliating cyberattacks, the imperative in Congress and the White House to do something — anything — in the name of improving cybersecurity was powerful.

But only the most cynical observers thought the results would be this bad.

f

t



68



V

“The bill is all the worst parts” of the different cybersecurity bills negotiated in recent months, Nathan White, senior legislative manager for Access Now, told *The Intercept*. “It was negotiated in secret. ... It’s a sneaky

f

t



68



Because of the last-minute timing, members of Congress “are not even going to know what they’re passing,” White said. “We don’t have time to get an informed vote, they’re pulling a fast one on the Senate.”

And the White House is reportedly on board. According to a [leaked document](#) published by Dustin Volz of Reuters, titled “Summary administration priorities for CISA”, the White House’s priorities line up with the new version of the bill — despite the fact that the administration threatened a veto over very similar legislation in 2013.

[According to](#) several technologists, information sharing isn’t a real solution to preventing cyberattacks. The best defense is better cyber hygiene.

“When you’ve got an epidemic, the answer is you should be washing your hands every time you use the bathroom. It’s just not a sexy thing to say,” Lee Tien, senior staff attorney at the Electronic Frontier Foundation, told *The Intercept* last January following President Obama’s State of the Union address, which focused heavily on cybersecurity.

Some opposition to the new bill has emerged among digital rights-supporting lawmakers and organizations, both Democratic and Republican. But they face off against the immensely powerful intelligence committees in the House and the Senate, congressional leadership, and the White House.

“Members of Congress are intentionally kept in dark so we don’t have time to rally opposition to particular measures,” Libertarian-leaning Rep. Justin Amash, R-Mich., [wrote on Twitter](#).

Rep. Zoe Lofgren, D-Calif., warned that the bill would “accomplish little more than increased unwarranted surveillance of U.S. persons, sharing private information with prosecutors and feeding the NSA dragnet.”

“This ‘cybersecurity’ bill was a bad bill when it passed the Senate and it is an even worse bill today,” said Sen. Ron Wyden, D-Ore. “Americans deserve policies that protect both their security and their liberty. This bill fails on both counts. Cybersecurity experts [say](#) CISA will do little to prevent



68




Overall, there was never much hope among the conservative groups. “We certainly would have liked more time to bring this issue to the attention of libertarians and conservatives. Unfortunately, the way the final bill was conferenced — keeping Chairman McCaul out of any substantive discussions and disregarding many of his concerns around the reconciliation process — moved it quicker than we anticipated,” wrote Ryan Hagemann of the Niskanen Center in an email to *The Intercept*.



CONTACT THE AUTHOR:



Jenna McLaughlin

 jenna.mclaughlin@theintercept.com

 [@JennaMC_Laugh](https://twitter.com/JennaMC_Laugh)

  16 Comments



68

