# What is SS7?

- Signaling System 7 is the set of protocols and systems used worldwide for:
  - Establishing/managing phone calls on landline and 2G/3G phones
  - Enabling Short Message Service (SMS) text messaging
  - Supports services like: 800 numbers, number portability, calling cards
- **5+ billion people use SS7; U.S. carriers use billions of SS7 messages/day**
  - **Issue 1**: **SS7 assumes trust between phone carriers worldwide**
  - **Issue 2: Many "bad actors" / "phone hackers" have access to SS7**
  - **Issue 3: Limited security controls are in place to prevent SS7 exploits**

**~ 7.7 billion cell phone subscriptions (world pop = 7.6 B!)**

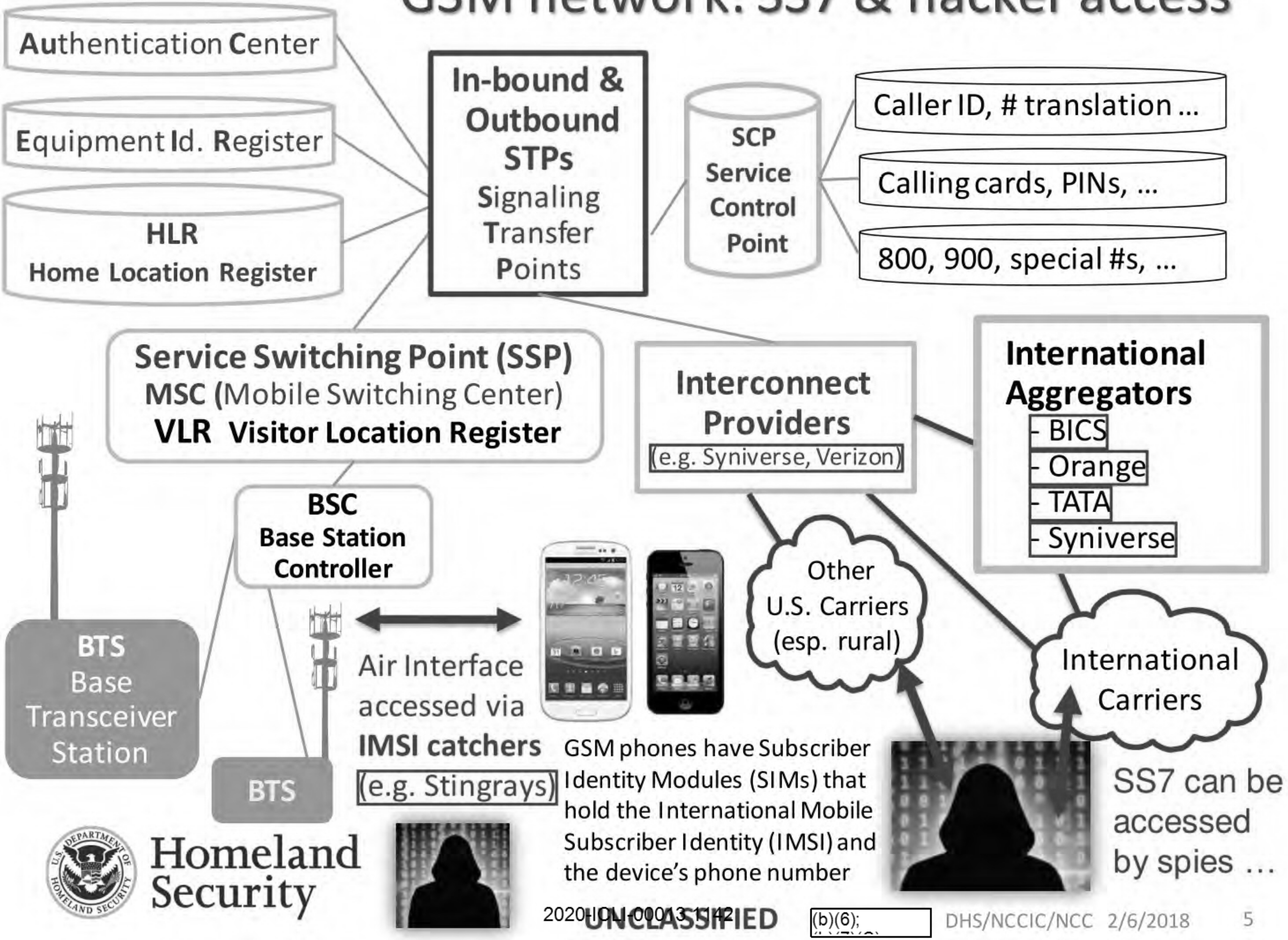
**SS7 has more users than Internet*, but is less secure!**

**Significant, undetected exploits are possible**

Homeland Security

* 2017 ITU estimate: 3.5 billion Internet users worldwide

# GSM network: SS7 & hacker access



Authentication Center

Equipment Id. Register

HLR
Home Location Register

In-bound & Outbound STPs
Signaling Transfer Points

SCP
Service Control Point

Caller ID, # translation …

Calling cards, PINs, …

800, 900, special #s, …

Service Switching Point (SSP)
MSC (Mobile Switching Center)
VLR Visitor Location Register

Interconnect Providers
(e.g. Syniverse, Verizon)

International Aggregators
- BICS
- Orange
- TATA
- Syniverse

BSC
Base Station Controller

BTS
Base Transceiver Station

BTS

Air Interface accessed via **IMSI catchers** (e.g. Stingrays)

Other U.S. Carriers (esp. rural)

International Carriers

GSM phones have Subscriber Identity Modules (SIMs) that hold the International Mobile Subscriber Identity (IMSI) and the device's phone number

SS7 can be accessed by spies …

Homeland Security

# 2008 - 2016: Examples of SS7 risks in media

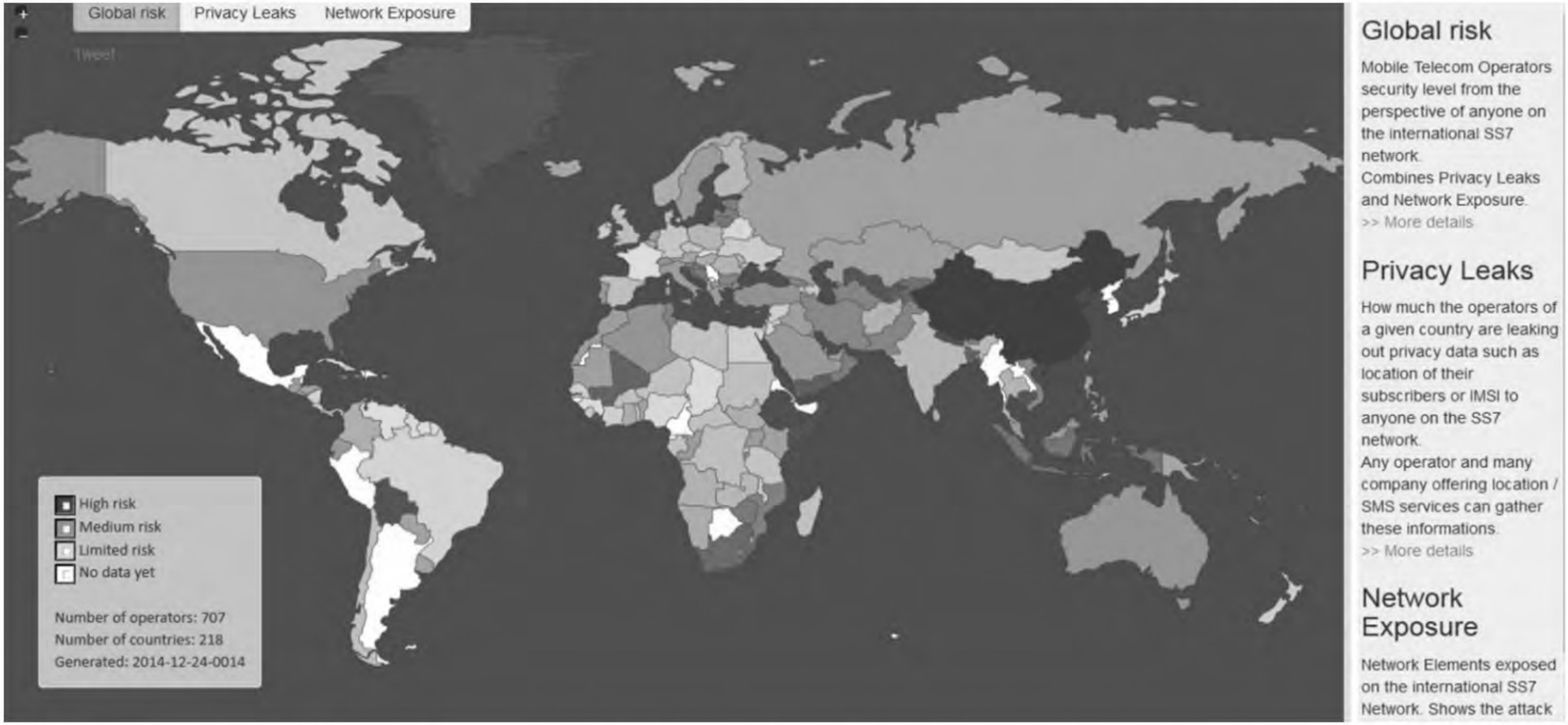
- **2008**: Chaos Communications Congress (CCC) – Tobias Engel: “Locating Mobile Phones using Signalling System #7” https://events.ccc.de/congress/2008/Fahrplan/attachments/1262_25c3-locating-mobile-phones.pdf
- 2011: CCC - Karsten Nohl – Exploiting calls + SMS* https://www.youtube.com/watch?v=ZrbatnnRxFc
- 2013: K. Nohl on SIM* risks http://michaelkreil.github.io/30c3-slides/slides_jpeg/saal1/2013-12-27T17-25-51.jpg
- **2014**: Year of more detailed risk explanations to public – greater focus at CCC
  - August - Washington Post: “*For sale: Systems that can secretly track where cellphone users go around the globe*” www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html
  - December - CCC (31c3) had three talks on cell phone SS7 related vulnerabilities
  - ZDNet “*Invasive phone tracking: New SS7 research blows the lid off mobile security*” www.zdnet.com/article/invasive-phone-tracking-new-ss7-research-blows-the-lid-off-personal-security/
- 2015: 60 Minutes Australia’s episode on SS7 and IMSI*-catcher risks www.news.com.au/technology/gadgets/the-end-of-privacy-as-we-know-it-60-minutes-uncovers-huge-mobile-phone-security-vulnerabilities/story-fn6vihic-1227485884359
- **2016: 60 Minutes “Hacking Your Phone” episode aired in USA** (aired 4/17/16)
  - Daily Beast reporting/reaction on SS7 phone issues and A/S Ozment’s hearing www.thedailybeast.com/articles/2016/04/23/here-s-why-anyone-could-hack-your-phone.html

Homeland Security

* SMS = Short Message Service IMSI = International Mobile Subscriber Identity
SIM = subscriber identity module or subscriber identification module [see slide notes for more details]

# 2014: SS7 risk awareness – SS7Map Global Risk

SS7Map assessed how well cellphone companies were safeguarding subscriber data. **The US was classified as a "medium risk".**



■ High risk
▩ Medium risk
▨ Limited risk
□ No data yet

Number of operators: 707
Number of countries: 218
Generated: 2014-12-24-0014

Global risk

Mobile Telecom Operators security level from the perspective of anyone on the international SS7 network.
Combines Privacy Leaks and Network Exposure.
>> More details

Privacy Leaks

How much the operators of a given country are leaking out privacy data such as location of their subscribers or IMSI to anyone on the SS7 network.
Any operator and many company offering location / SMS services can gather these informations.
>> More details

Network Exposure

Network Elements exposed on the international SS7 Network. Shows the attack

[Note: P1 Security (a French firm) produced this map; see http://ss7map.p1sec.com ]

# 2015 threat example: OPM data breach

- Office of Personnel Management (OPM) data breaches impacted those who applied for clearances along with their associates (over 21 million people's personal data compromised)
- **Compromised data included:**
  - Age and Address
  - Relationships
  - Home/work phone numbers
  - **Cell phone numbers**

- In 2015, **Chinese government arrested some hackers** it says were connected to the breach of OPM's database
- In 2017, the **FBI arrested a Chinese national** connected to the Sakura malware used in the OPM data breach

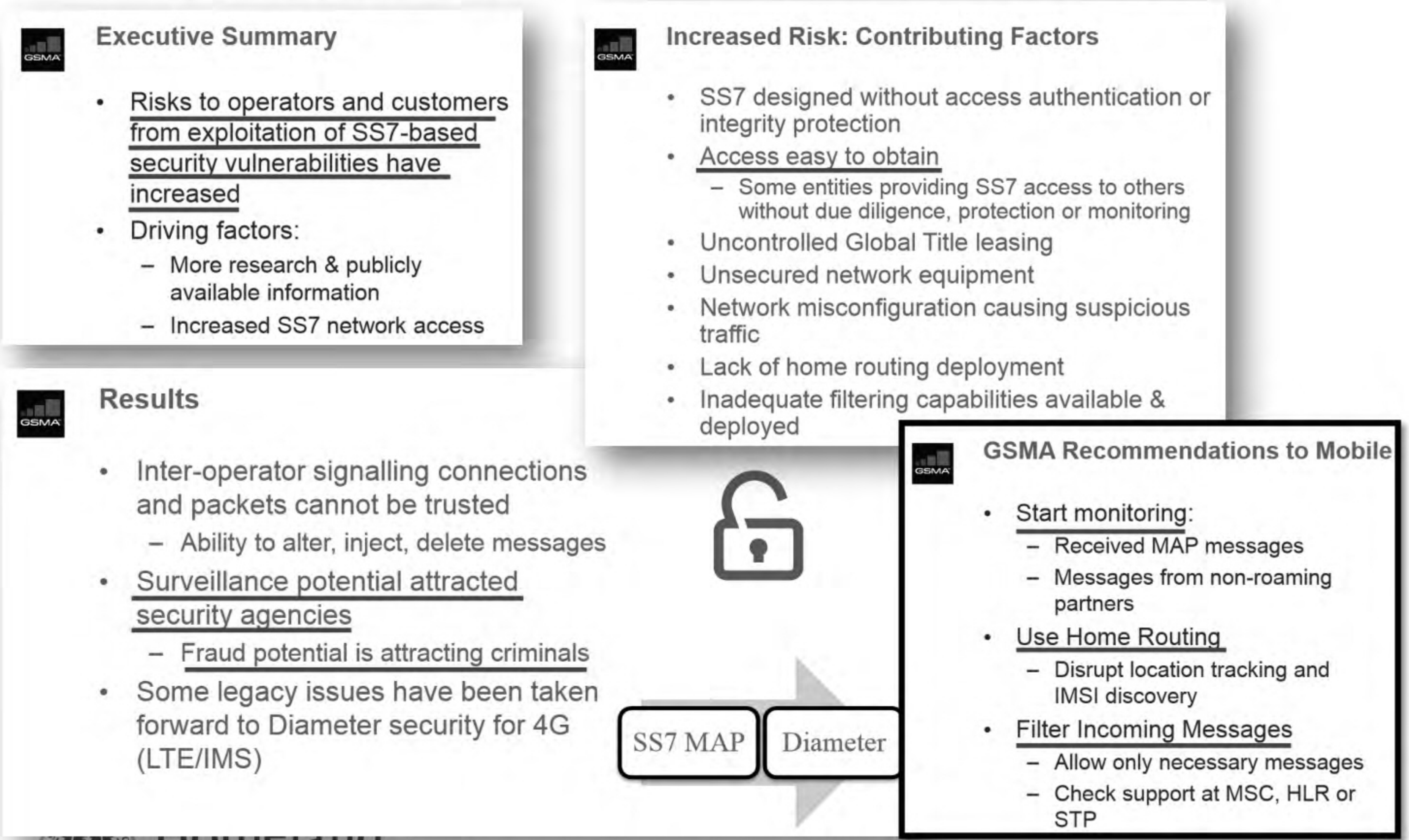
Homeland Security

# Reported 2015 SS7 anomalous traffic Possibly related to OPM breach

(b)(7)(E)

Note: This is preliminary data and does not represent all suspicious SS7 traffic that occurred during the summer of 2015

# 2016 GSMA brief on SS7 Interconnect Security



### Executive Summary

- Risks to operators and customers from exploitation of SS7-based security vulnerabilities have increased
- Driving factors:
  - More research & publicly available information
  - Increased SS7 network access

### Increased Risk: Contributing Factors

- SS7 designed without access authentication or integrity protection
- Access easy to obtain
  - Some entities providing SS7 access to others without due diligence, protection or monitoring
- Uncontrolled Global Title leasing
- Unsecured network equipment
- Network misconfiguration causing suspicious traffic
- Lack of home routing deployment
- Inadequate filtering capabilities available & deployed

### Results

- Inter-operator signalling connections and packets cannot be trusted
  - Ability to alter, inject, delete messages
- Surveillance potential attracted security agencies
  - Fraud potential is attracting criminals
- Some legacy issues have been taken forward to Diameter security for 4G (LTE/IMS)

### GSMA Recommendations to Mobile

- Start monitoring:
  - Received MAP messages
  - Messages from non-roaming partners
- Use Home Routing
  - Disrupt location tracking and IMSI discovery
- Filter Incoming Messages
  - Allow only necessary messages
  - Check support at MSC, HLR or STP

(b)(6); (b)(7)(C)

# 2016: Telenor incident / US networks have similar risks!

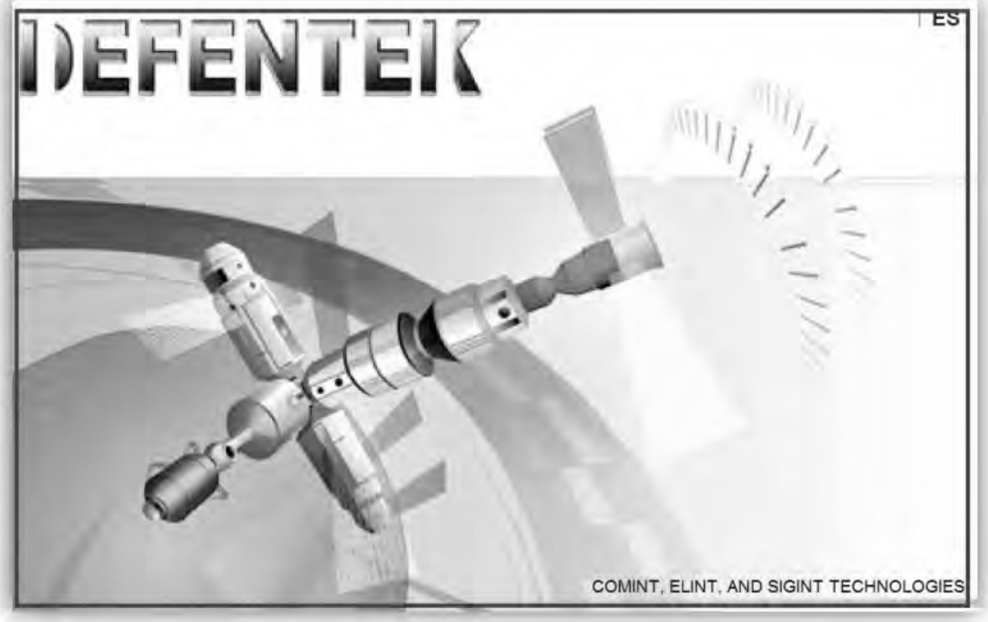
(b)(7)(E)

Note: used by permission of source

(b)(7)(E)

(b)(7)(E)

# 2016: Cell phone exploits advertised on the Internet: note … this site is no longer available



From www.defentek.com:

> “The ***Infiltrator*** is a … solution for collecting, analyzing and presenting the status of any mobile user status & location. The ***Infiltrator*** gives a clear location and movement of anyone anywhere in the world. Even if the SIM card is switched out, we are actually tracking the handset thereafter. Additional modules allows to remotely activate the speaker on the handset and capture all of the surrounding conversation anywhere in the world where the hand set is located, and no matter how many times the SIM card is switched or replaced.”

Homeland Security

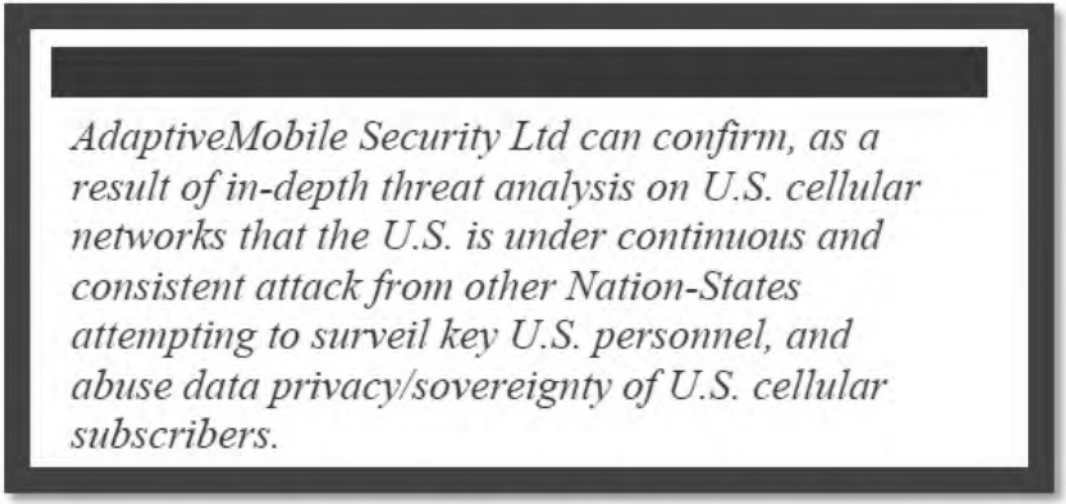
(b)(7)(E)

Note: used by permission of source

(b)(7)(E)

Note: Derived/used by permission of source

# April-May 2017: DHS Mobile Device Security Report



[redacted]

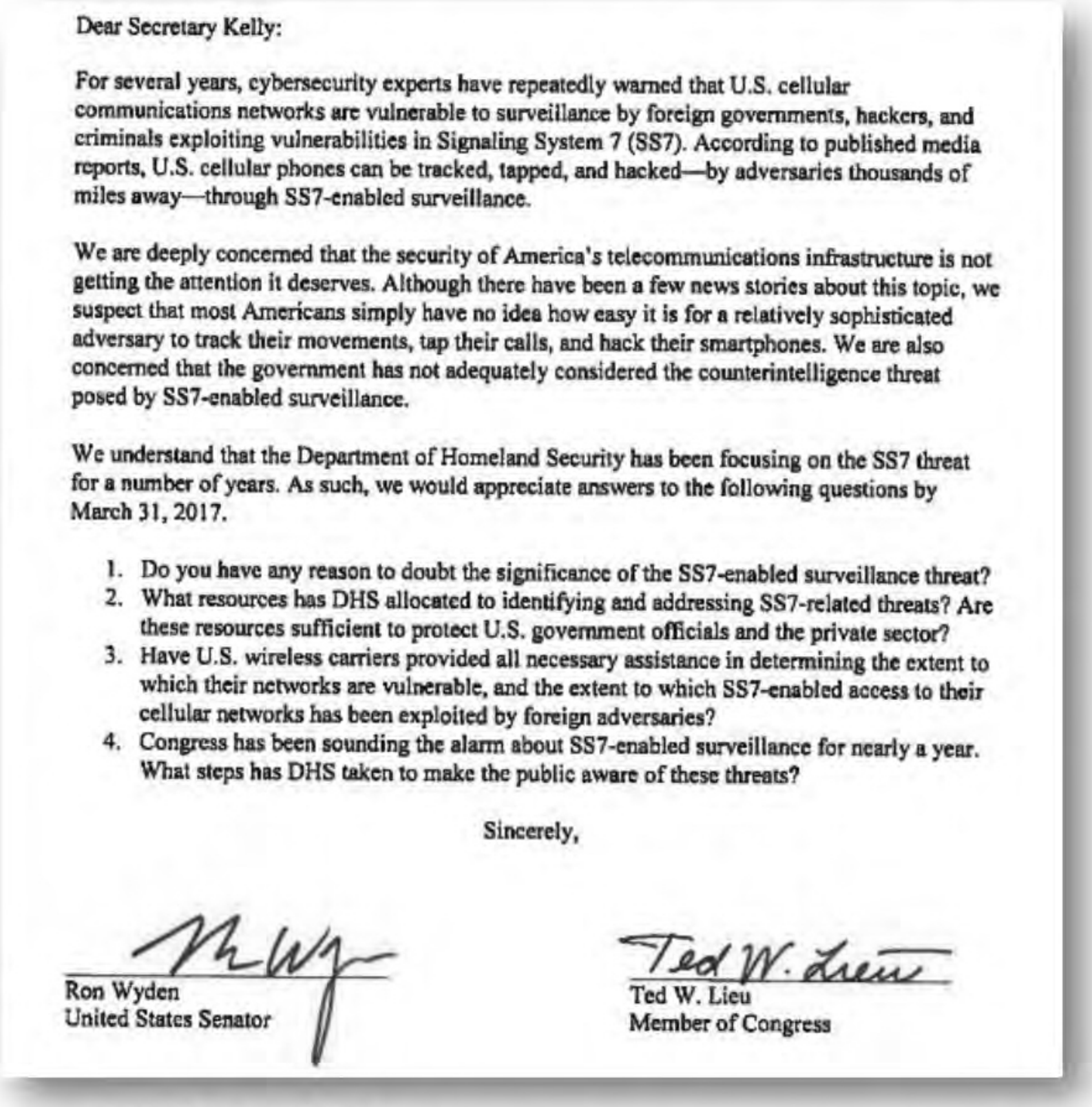
*AdaptiveMobile Security Ltd can confirm, as a result of in-depth threat analysis on U.S. cellular networks that the U.S. is under continuous and consistent attack from other Nation-States attempting to surveil key U.S. personnel, and abuse data privacy/sovereignty of U.S. cellular subscribers.*

- *"Threats to the Government's use of mobile devices are real and exist across all elements of the mobile ecosystem."*
- *"Gaining unauthorized access to the core SS7 or Diameter network is a risk since there are tens of thousands of entry points worldwide, many of which are controlled by countries or organizations that support terrorism or espionage."*
- *"A number of threats against SS7 have been publicly described, including the ability to determine the physical location of cellular mobile devices, disrupt phone service from individual phones to entire networks, intercept or block SMS text messages, and redirect or eavesdrop on voice conversations."*

# March 2017: Congressional letter to DHS S1

*"… According to published media reports, U.S. cellular phones can be tracked, tapped, and hacked …*

*We are deeply concerned that the security of America's telecommunications infrastructure is not getting the attention it deserves. …"*



Dear Secretary Kelly:

For several years, cybersecurity experts have repeatedly warned that U.S. cellular communications networks are vulnerable to surveillance by foreign governments, hackers, and criminals exploiting vulnerabilities in Signaling System 7 (SS7). According to published media reports, U.S. cellular phones can be tracked, tapped, and hacked—by adversaries thousands of miles away—through SS7-enabled surveillance.

We are deeply concerned that the security of America's telecommunications infrastructure is not getting the attention it deserves. Although there have been a few news stories about this topic, we suspect that most Americans simply have no idea how easy it is for a relatively sophisticated adversary to track their movements, tap their calls, and hack their smartphones. We are also concerned that the government has not adequately considered the counterintelligence threat posed by SS7-enabled surveillance.

We understand that the Department of Homeland Security has been focusing on the SS7 threat for a number of years. As such, we would appreciate answers to the following questions by March 31, 2017.

1. Do you have any reason to doubt the significance of the SS7-enabled surveillance threat?
2. What resources has DHS allocated to identifying and addressing SS7-related threats? Are these resources sufficient to protect U.S. government officials and the private sector?
3. Have U.S. wireless carriers provided all necessary assistance in determining the extent to which their networks are vulnerable, and the extent to which SS7-enabled access to their cellular networks has been exploited by foreign adversaries?
4. Congress has been sounding the alarm about SS7-enabled surveillance for nearly a year. What steps has DHS taken to make the public aware of these threats?

Sincerely,

Ron Wyden
United States Senator

Ted W. Lieu

Ted W. Lieu
Member of Congress

Homeland Security

# June 2017 - VoLTE is vulnerable

## BleepingComputer June 12, 2017 article:

"A team of researchers from French company P1 Security has detailed a long list of issues with the 4G VoLTE telephony, a protocol that has become quite popular all over the world in recent years and is currently in use in the US …

VoLTE stands for Voice Over LTE – where LTE stands for Long-Term Evolution and is a high-speed wireless communication for mobile phones and data terminals, based on older GSM technology.

Researchers say they identified both "active" vulnerabilities (that require modifying special SIP packets) and "passive" vulnerabilities (that expose data via passive network monitoring or do not require any SIP packet modification)."

**Note: FirstNet uses VoLTE technology**

**Sources**: (1) https://www.bleepingcomputer.com/news/security/hackers-can-spoof-phone-numbers-track-users-via-4g-volte-mobile-technology/
(2) P1 Security published "Subscribers remote geolocation and tracking using 4G VoLTE enabled Android phone" in June 2017. https://www.sstic.org/media/SSTIC2017/SSTIC-actes/remote_geolocation_and_tracing_of_subscribers_usin/SSTIC2017-Article-remote_geolocation_and_tracing_of_subscribers_using_4g_volte_android_phone-le-moal_ventuzelo_coudray.pdf

# Cellular Threats

(b)(7)(E)

# Cellular Threats

(b)(7)(E)

Note: used by permission of source

## Cellular Threats

(b)(7)(E)

Note: used by permission of source

# NCC Cellular Pilot Update: "Overwatch" in NCR

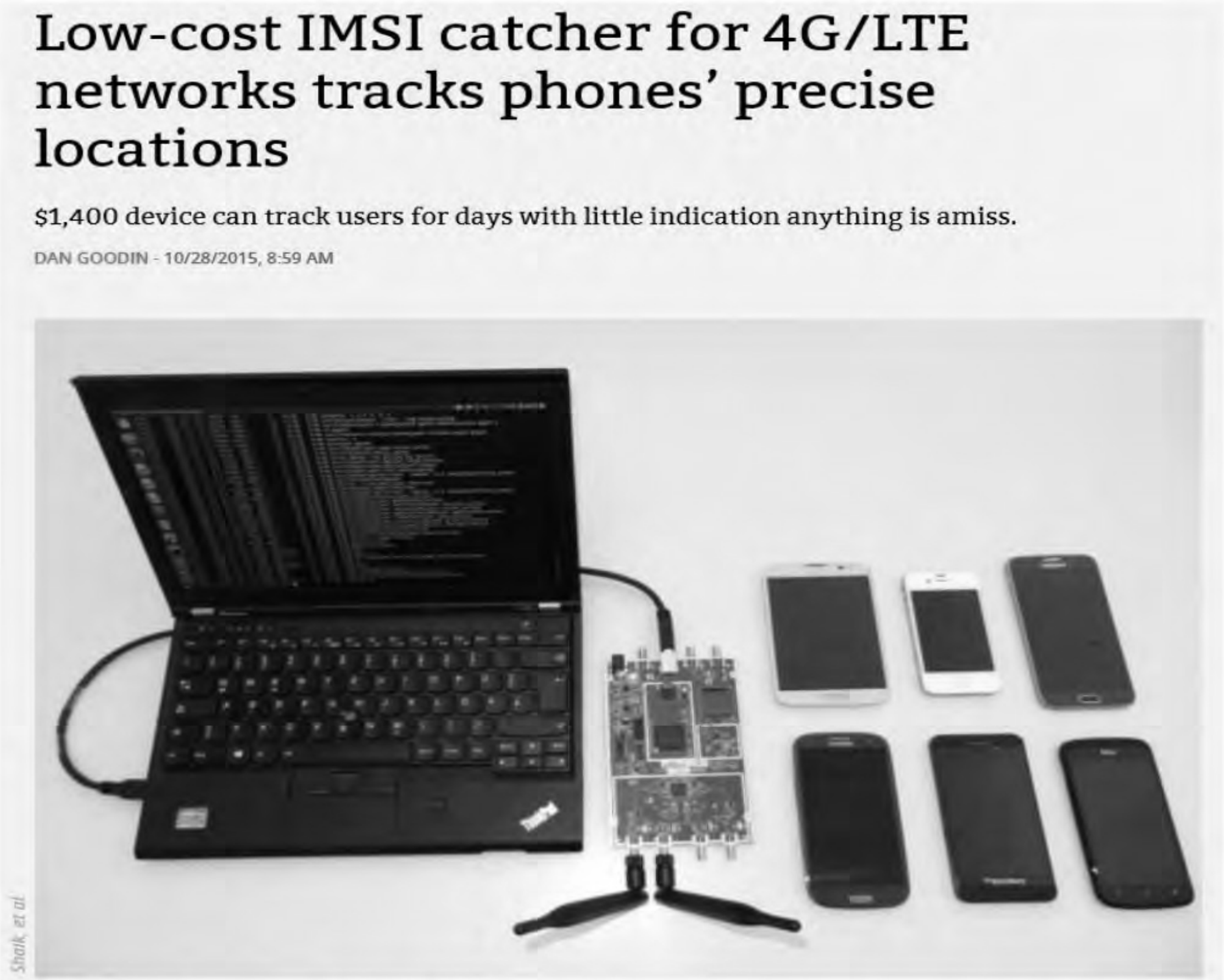
(b)(7)(E)

## Sensors detect IMSI catchers

- NCC Pilot detects, characterizes, and geo-locates legitimate and rogue cellular base stations (also known as IMSI catchers) in the National Capital Region
- Reportedly: *"first and only strategic real-time IMSI catcher detection system"*

(b)(7)(E)

# Threat 1: Low-cost rogue cellular base stations



## Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations

$1,400 device can track users for days with little indication anything is amiss.

DAN GOODIN - 10/28/2015, 8:59 AM

Shaik, et al.

"The equipment can cause all LTE-compliant phones to leak their location to within a 32- to 64-foot radius … operating a rogue base station… total cost" … about $1,400

https://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/

* IMSI = International Mobile Subscriber Identity

Homeland Security

# Threat 2: Sophisticated rogue cellular base stations

- Example: (b)(7)(E) (b)(7)(E) can intercept, record, & track cell phones/devices
- Range: hundreds of meters
- (b)(7)(E) also (b)(7)(E) "IMSI* catchers"
  - Detect mobile phones & extract their identities (e.g. IMSIs)
  - Can be wearable or used in cars or airborne platforms
  - Can be used with direction finders
  - Can also exploit phones on CDMA* networks and GSM* networks

Sources: (b)(7)(E) and other pages on that site

* **CDMA** = Code Division Multiple Access; **GSM** = Global System for Mobile Communications; **IMSI** = International Mobile Subscriber Identity;

Homeland Security

# NCC Rogue Cellular Pilot findings: (b)(7)(E)

## August 23, 2016: Detected likely IMSI catcher monitoring/tracking phones (b)(7)(E)

- Potential IMSI catcher emulating an existing tower on (b)(7)(E)

(b)(7)(E)

# Pilot findings – (b)(7)(E) [redacted] rogue cell in VA

(b)(7)(E) [redacted]

# Possible rogue cell (b)(7)(E) – 30 Aug 2017

(b)(7)(E)

(b)(7)(E)

[redacted]

# Conclusions / General Way Ahead

- Government & industry must continue to work together to address threats
  - Tracking and monitoring of leaders, staff, and public; (b)(7)(E)

(b)(7)(E)

- Don't take cell phones into sensitive meetings (or use Faraday bags/boxes)
- Users can mitigate their risks through exploit resilient end devices and Apps
- Can use phone service contracts that require SS7 monitoring/filtering/reporting
- Need sophisticated monitoring/filtering (b)(7)(E)

Homeland Security

Need **comprehensive** monitoring/blocking of malicious traffic and trust based on **verification**

**U.S. Department of Homeland Security**
Washington, DC 20528

Homeland
Security

December 4, 2017

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

Thank you for your August 24, 2017 letter. Acting Secretary Duke asked that I respond on her behalf.

For specific responses to each of your questions, please refer to the enclosure. To address your specific concern related to U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO) utilizing cell-site simulators, I can confirm that ICE/ERO does not use cell-site simulators for the purpose of civil immigration law enforcement. While ICE/ERO's primary mission is to enforce the Nation's civil immigration laws, individual ERO officers may participate in Joint Task Forces with federal, state, and local law enforcement partners, in furtherance of our shared public safety mission. Such Joint Task Forces may employ various technologies, including cell-site simulator technology, to pursue individuals suspected of engaging in criminal activity. However, such use must be conducted in a manner that protects rights afforded by the U.S. Constitution, and in compliance with applicable statutory authorities.

While cell-site simulators are used by several Components of the Department of Homeland Security (DHS), no Component is using this technology for the purpose of civil immigration enforcement. (b)(7)(E)

(b)(7)(E)

U.S. Customs and Border Protection (CBP) has made limited use of cell-site simulators.

(b)(7)(E)

The United States Secret Service (USSS) also uses cell-site simulators (b)(7)(E)

(b)(7)(E)

The DHS Components that use cell-site simulators do so in a manner that is consistent with DHS Policy Directive 047-02, *Department Policy Regarding the Use of Cell-Site Simulator Technology*, dated October 19, 2015, which closely aligns with the Department of Justice's policy guidance regarding the use of cell-site simulator technology. Under current policy, absent exigent circumstances under the Fourth Amendment or other exceptional circumstances where the law does not require a search warrant, operators must obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or applicable state equivalent).

The technology is typically used to either locate a subject using their mobile device, or to determine which mobile device (i.e., smartphone) a subject is carrying. In the context of criminal investigations, (b)(7)(E)

(b)(7)(E)

(b)(7)(E) Devices are always able to dial 911 without any disruption of service. DHS remains committed to ensuring law enforcement practices concerning the collection or retention of data are lawful and respect the important privacy interests of individuals.

Thank you again for your letter and interest in this important matter. The cosigners of your letter will receive separate, identical responses. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

James D. Nealon
Assistant Secretary for International Affairs
Office of Strategy, Policy, and Plans

Enclosure

## The Department of Homeland Security's Response to Senator Al Franken's August 24, 2017 Letter

1. **Policy Directive 047-02 "applies to the use of CSS technology inside the United States in furtherance of criminal investigations." According to ICE, CSS devices are used "in support of criminal investigations requiring judicial process, and not for administrative violations under the Immigration and Nationality Act." ICE has also stated that ICE Enforcement and Removal Operations (ERO) "does not use cell-site simulators for the purpose of civil immigration enforcement."**

   a. **In the Department's use of CSS technology for criminal investigations, does DHS distinguish between the seriousness of criminal offenses in determining whether to deploy CSS technology? If so, how?**

   Neither the Department of Homeland Security (DHS) nor its Components have specifically prioritized criminal offenses for this purpose.

   U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) does not have a protocol designating a specific list of priority violations. In the event of limited resources, ICE HSI prioritizes cell-site simulator (CSS) deployments based on mission needs.

   (b)(7)(E)

   b. **The Department's response to Senator Wyden's May 23, 2017 letter confirmed that ERO does not use CSS devices for administrative immigration enforcement. Does any other Component within the Department use CSS technology pursuant to non-criminal investigations within the United States.**

   Within DHS, ICE HSI and USSS are the predominant users of CSS devices, and CBP has made limited use of this technology. No DHS Component uses CSS technology for the purpose of civil immigration enforcement or other "non-criminal" investigations.

2. **Policy Directive 047-02 states that "[a]ffected DHS Components may issue additional specific guidance consistent with this policy." Please provide copies of all such additional specific guidance, if any, issued by DHS's immigration enforcement Components.**

   ICE HSI has issued internal guidance that is consistent with the October 19, 2015 DHS Policy Directive 047-02, *Department Policy Regarding the Use of Cell-Site Simulator Technology*, as well as the Department of Justice's *Guidance on the Use of Cell-Site Simulator Technology.* CBP is in the process of developing internal operational policy governing the use of CSS technology.

3. **Policy Directive 047-02 provides that DHS Components shall implement an auditing program to ensure that data collected by CSS technology is deleted following the completion of a mission, upon location of a target, and upon the identification of a target. Are such audits performed by Components that use CSS technology for immigration enforcement? If not, why?**

   a. **If so, how frequently are such audits performed?**
   b. **If so, what have such audits revealed about DHS Components' data collection, retention, and disposal practices?**

   DHS Components do not use CSS technology for administrative immigration violations.

4. **Policy Directive 047-02 provides that "DHS is committed to ensuring that law enforcement practices concerning the collection and retention of data are lawful and respect the important privacy interests of individuals." Furthermore, in response to Senator Wyden's letter, ICE stated that ICE Homeland Security Investigations operates CSS devices "in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information."**

   a. **Aside from Policy Directive 047-02, what "rules, policies, and laws" apply to information collected through the use of CSS technology? In particular, what "rules, policies, and laws" apply to information about noncitizens obtained through the use of CSS technology?**

   DHS uses CSS devices in a manner consistent with the requirements and protections of the Constitution, including the Fourth Amendment and applicable statutory authorities, including the Pen Register Statute (18 U.S.C. §§ 3121 *et seq.*). DHS Components' CSS use is also guided by DHS Policy Directive 047-02 and Component policy.

   Pursuant to Department Policy, absent exigent circumstances under the Fourth Amendment or other exceptional circumstances where the law does not require a search warrant, operators are required to obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or applicable state equivalent). Nationality and/or citizenship are not considered when deploying these devices; DHS Components deploy the devices only with probable cause supporting that an individual is suspected of committing a criminal violation.

Information that ICE HSI collects from CSS devices that is relevant to an investigation is recorded in Reports of Investigations, which are stored in the appropriate investigative file and retained in accordance with the applicable federal records schedule. Information that is not relevant to an investigation is not retained. Any information that ICE collects from CSS devices pertaining to U.S. citizens or Lawful Permanent Residents (LPRs) is used and disclosed in accordance with the DHS ICE – 009 External Investigations System of Records Notice.[1] Finally, any information ICE obtains from CSS devices pertaining to individuals who are neither U.S. citizens nor LPRs is handled in accordance with the Fair Information Practice Principles as outlined in DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*.[2] In addition to those protections, any information ICE obtains from these devices pertaining to individuals that may have applied or been granted U Nonimmigrant Status, T Nonimmigrant status, or protections under the *Violence Against Women Act* are handled in accordance with 8 U.S.C. Section 1367.

**b. Section 14 of President Trump's Executive Order, entitled *Enhancing Public Safety in the Interior of the United States*, seeks to remove Privacy Act protections from immigrants who are not U.S. citizens or permanent residents. What effect does Section 14 of the President's January 25, 2017 Executive Order have on the Department's data collection and disposal policies, including but not limited to those laid out in Policy Directive 047-20?**

Section 14 of President Trump's Executive Order, *Enhancing Public Safety in the Interior of the United States*, will not change how DHS and, specifically, ICE collects or disposes of data obtained through CSS devices.

**5. Policy Directive 047-02 provides that an application or supporting affidavit should inform the court that the target cell phone and other cell phones in the area of the CSS device might experience a temporary disruption of service from the service provider. In response to Senator Wyden's letter, ICE stated that "[d]uring use of cell-site simulators, interference with non-targeted mobile devices is virtually non-existent." ICE also stated that "[i]n all circumstances, devices are always able to dial 911 without any disruption of service." Please describe, in detail, how DHS knows this to be the case "in all circumstances."**

[1] *See* DHS/ICE – External Investigations System of Records Notice, (75 FR 404, Jan. 5, 2010), *available at*: https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31269.htm.

[2] https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.

**a. Have DHS employees (rather than manufacturers or third parties) tested the CSS technology the Department uses to measure the interference caused to nearby phones? If so, please provide a copy of all testing reports or other documentation related to device and network interference caused by CSS technology.**

Neither ICE nor USSS has funded independent interference testing. Components rely on manufacturer specifications and their extensive experience with the technology in the field.

With respect to your question about disruption of service, when CSS devices are in use, (b)(7)(E)

DHS is not aware of any complaints or reports of network interference or disruption from the CSS technology used by DHS.

**6. Does DHS maintain a record of which components possess CSS technology; how many CSS devices each component has; the makes and models of CSS devices used by each component; and when, where, and for how long the devices are used for immigration enforcement? If so, please provide a copy of such records.**

DHS does not maintain a centralized repository of this information. Currently, ICE HSI has (b)(7)(E) CSSs are used in support of criminal investigations, requiring judicial process, and are not utilized for administrative violations under the Immigration and Nationality Act. The makes and models of CSS equipment utilized by DHS are considered law enforcement sensitive. DHS personnel may be made available to discuss equipment specifics should a briefing be deemed necessary.

**7. Does DHS maintain a record of how many individuals have been located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology? If so, please provide a copy of such records and state how many of the individuals located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology have been arrested for a crime, convicted of a crime, and convicted of a violent crime.**

DHS does not use CSS for administrative immigration violations.

(b)(7)(E)

**8. Does DHS deploy CSS technology for immigration enforcement purposes along the nation's borders? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.**

No.

**9. Does DHS deploy CSS technology during interior immigration enforcement? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.**

No.

Page 1176

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1177

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1178

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1179

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1180

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1181

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1182

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1183

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1184

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1185

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

United States Senate

WASHINGTON, DC 20510

August 24, 2017

The Honorable Elaine C. Duke
Acting Secretary of Homeland Security
U.S. Department of Homeland Security
Washington, DC 20528

Dear Acting Secretary Duke:

In light of reports that federal authorities deployed cell-site simulator (CSS) technology during an immigration raid, we write to request additional information about the Department of Homeland Security's (DHS) use of these powerful surveillance devices in immigration enforcement actions.[1] While we appreciate the need for federal law enforcement agencies to locate and track dangerous suspects, we are concerned that using CSS technology during immigration enforcement actions poses a significant risk to privacy and civil liberties.

CSS devices—commonly known as "stingrays" or International Mobile Subscriber Identity Catcher devices (IMSI-catchers)—are portable surveillance devices that mimic cellphone towers and compel affected mobile phones to reveal their location and registration information. In recognition of the important privacy concerns raised by the use of CSS technology, in October 2015 DHS issued a policy directive on the Department's use of such devices (Policy Directive 047-02).[2] The directive "applies to the use of CSS technology inside the United States in furtherance of criminal investigations," and it requires DHS's law enforcement components to obtain a search warrant supported by probable cause before deploying CSS technology. The directive also imposes some appropriate limits on cell phone data collection and retention. However, because the directive's scope only applies to criminal investigations, it does not apply to the administrative investigations that make up a substantial portion of DHS's immigration enforcement actions.

A recently published federal search warrant affidavit revealed publicly for the first time that an Immigration and Customs Enforcement (ICE) officer used a CSS device to track the location of an undocumented immigrant.[3] In that particular case, according to the affidavit, DHS was conducting a criminal investigation of the undocumented immigrant for violation of 8 U.S.C. §1326(a).[4] Accordingly, a federal judge issued a warrant authorizing, among other things, the use of a CSS device.

[1] Alvaro M. Bedoya, *Deportation Is Going High-Tech Under Trump*, THE ATLANTIC, June 21, 2017, *at* https://www.theatlantic.com/technology/archive/2017/06/data-driven-deportation/531090/.
[2] U.S. Department of Homeland Security, Policy Directive 047-02, Department Policy Regarding the Use of Cell-Site Simulator Technology (Oct. 19, 2015), *at* https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.
[3] Robert Snell, *Feds use anti-terror tool to hunt the undocumented*, DETROIT NEWS, May 18, 2017, *at* http://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/.
[4] Search Warrant Affidavit for *The Cellular Device Assigned Call Number (XXX) XXX-XXXX*, Eastern District of Michigan, no. 2:17-mc-50368-01 (2017), *at* https://www.documentcloud.org/documents/3727182-CSS1.html.

In response to questions raised by Senator Wyden,[5] ICE clarified that it deploys CSS devices only in support of "criminal investigations requiring judicial process," and that it "does not use cell-site simulators for the purpose of civil immigration enforcement."[6] ICE also explained that it continues to apply the limitations set forth in Policy Directive 047-02 to its use of CSS technology. However, significant questions remain about the Department's use of CSS technology for immigration enforcement purposes, such as the extent of the technology's deployment in our cities and neighborhoods, and what additional safeguards are in place to protect the privacy and civil liberties of our immigrant communities. In an effort to gain a better understanding of how DHS's immigration enforcement officers are using CSS technology, we respectfully request that you provide individual responses to each of the following questions:

1. Policy Directive 047-02 "applies to the use of CSS technology inside the United States in furtherance of criminal investigations." According to ICE, CSS devices are used "in support of criminal investigations requiring judicial process, and not for administrative violations under the Immigration and Nationality Act." ICE has also stated that ICE Enforcement and Removal Operations (ERO) "does not use cell-site simulators for the purpose of civil immigration enforcement."

    a. In the Department's use of CSS technology for criminal investigations, does DHS distinguish between the seriousness of criminal offenses in determining whether to deploy CSS technology? If so, how?

    b. The Department's response to Senator Wyden's May 23, 2017 letter confirmed that ERO does not use CSS devices for administrative immigration enforcement. Does any other component within the Department use CSS technology pursuant to non-criminal investigations within the United States?

2. Policy Directive 047-02 states that "[a]ffected DHS Components may issue additional specific guidance consistent with this policy." Please provide copies of all such additional specific guidance, if any, issued by DHS's immigration enforcement components.

3. Policy Directive 047-02 provides that DHS components shall implement an auditing program to ensure that data collected by CSS technology is deleted following the completion of a mission, upon location of a target, and upon the identification of a target. Are such audits performed by components that use CSS technology for immigration enforcement? If not, why?

    a. If so, how frequently are such audits performed?

    b. If so, what have such audits revealed about DHS components' data collection, retention, and disposal practices?

[5] Letter from Ron Wyden, U.S. Senator, to Thomas D. Homan, Acting Director of U.S. Immigration & Customs Enforcement (May 23, 2017), *at* https://www.wyden.senate.gov/download/?id=F268CF50-4BF1-41A4-860A-8CED078CAB4A&download=1.

[6] Letter from Thomas D. Homan, Acting Director of U.S. Immigration & Customs Enforcement, to Ron Wyden, U.S. Senator (Aug. 16, 2017), *at* https://assets.documentcloud.org/documents/3935329/88437-Signed-Response.pdf.

4. Policy Directive 047-02 provides that "DHS is committed to ensuring that law enforcement practices concerning the collection and retention of data are lawful and respect the important privacy interests of individuals." Furthermore, in response to Senator Wyden's letter, ICE stated that ICE Homeland Security Investigations operates CSS devices "in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information."

    a. Aside from Policy Directive 047-02, what "rules, policies, and laws" apply to information collected through the use of CSS technology? In particular, what "rules, policies, and laws" apply to information about noncitizens obtained through the use of CSS technology?

    b. Section 14 of President Trump's Executive Order, entitled *Enhancing Public Safety in the Interior of the United States*, seeks to remove Privacy Act protections from immigrants who are not U.S. citizens or permanent residents. What effect does Section 14 of the president's January 25, 2017 executive order have on the Department's data collection and disposal policies, including but not limited to those laid out in Policy Directive 047-02?

5. Policy Directive 047-02 provides that an application or supporting affidavit should inform the court that the target cell phone and other cell phones in the area of the CSS device might experience a temporary disruption of service from the service provider. In response to Senator Wyden's letter, ICE stated that "[d]uring use of cell-site simulators, interference with non-targeted mobile devices is virtually non-existent." ICE also stated that "[i]n all circumstances, devices are always able to dial 911 without any disruption of service." Please describe, in detail, how DHS knows this to be the case "in all circumstances."

    a. Have DHS employees (rather than manufacturers or third parties) tested the CSS technology the Department uses to measure the interference caused to nearby phones? If so, please provide a copy of all testing reports or other documentation related to device and network interference caused by CSS technology.

6. Does DHS maintain a record of which components possess CSS technology; how many CSS devices each component has; the makes and models of CSS devices used by each component; and when, where, and for how long the devices are used for immigration enforcement? If so, please provide a copy of such records.

7. Does DHS maintain a record of how many individuals have been located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology? If so, please provide a copy of such records and state how many of the individuals located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology have been arrested for a crime, convicted of a crime, and convicted of a violent crime.

8. Does DHS deploy CSS technology for immigration enforcement purposes along the nation's borders? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.

9. Does DHS deploy CSS technology during interior immigration enforcement? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.

Thank you for your prompt attention to this important matter.

Sincerely,

Al Franken
AL FRANKEN
United States Senator

RON WYDEN
United States Senator

Patrick Leahy
PATRICK LEAHY
United States Senator

Dick Durbin
RICHARD J. DURBIN
United States Senator