Written Testimony of Jonathan Mayer
Assistant Professor of Computer Science and Public Affairs, Princeton University

Before the Committee on Science, Space, and Technology
Subcommittee on Oversight
United States House of Representatives

June 27, 2018

Chairman Abraham, Ranking Member Beyer, and members of the Subcommittee, thank you for the opportunity to address communications security and privacy at today's hearing. I worked extensively on these topics during my recent service as Chief Technologist of the Federal Communications Commission Enforcement Bureau, and they have been an essential component of my academic research and teaching.

In last week's groundbreaking *Carpenter v. United States* decision, Chief Justice Roberts wrote that "cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society."[1] Smartphones are just a starting point—tablets, wristwatches, and cars are also increasingly connected to cellular networks. And the future is even more wireless—telemedicine, autonomous ground vehicles, and airborne drones are on the horizon. It is not hyperbole to acknowledge that the private sector, the public sector, and the American people depend on our wireless communications infrastructure.

The security and privacy safeguards for that infrastructure have not kept pace with its growing importance to the nation. Our wireless networks have significant cybersecurity vulnerabilities that could be exploited by criminals and foreign adversaries. And when law enforcement agencies seek to conduct investigations using wireless technology, the applicable federal law is imprecise, outdated, likely unconstitutional, and leaves police departments in legal limbo.

In this written testimony, I will begin by explaining how cell-site simulators function and what information they can obtain from smartphones and other mobile devices. I will also highlight several other serious cybersecurity vulnerabilities in the nation's wireless infrastructure that merit congressional attention and oversight activity.

Next, I will describe how criminals could use cell-site simulators to perpetrate offenses and how foreign intelligence services could use the same devices to conduct espionage against America's businesses and government institutions. Congress should take immediate action to address these threats by ensuring that, when it spends about a billion taxpayer dollars on wireless services and devices each year, it procures services and devices that implement cybersecurity best practices.

Finally, I will explain how law enforcement agencies nationwide are using cell-site simulators to conduct criminal investigations. I will also explain how, under current federal law, it is both a regulatory offense and a crime for a state, local, or tribal police department to operate a cell-site simulator. I agree with the bipartisan report issued by the Committee on Oversight and

[1] Carpenter v. United States, No. 16-402, 2018 WL 3073916, at *2 (U.S. June 22, 2018).

Government Reform in December 2016: Congress should establish a clear statutory framework for law enforcement use of cell-site simulators.[2]

I. Cybersecurity Vulnerabilities in the Nation's Wireless Infrastructure

Cellular connectivity is simply a form of radio communication. Smartphones and other mobile devices are radio transmitters and receivers, and cellular towers are radio base stations that are linked to telephone and internet infrastructure.[3] A mobile device maintains contact with multiple cellular towers in order to maximize service quality; it will automatically and seamlessly switch between towers depending on signal strength, resource availability, tower instructions, and other relevant factors. While cellular technology has radically improved since the earliest commercial networks in the 1980s, this fundamental design has remained and foreseeably will remain unchanged.

A. Cell-Site Simulators

Cell-site simulators, commonly dubbed "IMSI catchers," "Stingrays," or "Dirtboxes," are devices that exploit omissions and mistakes in the trust between mobile devices and cellular towers.[4] A cell-site simulator mimics a legitimate cellular tower and tricks nearby mobile devices into connecting to it. The cell-site simulator then takes advantage of the connection to extract information from those devices.

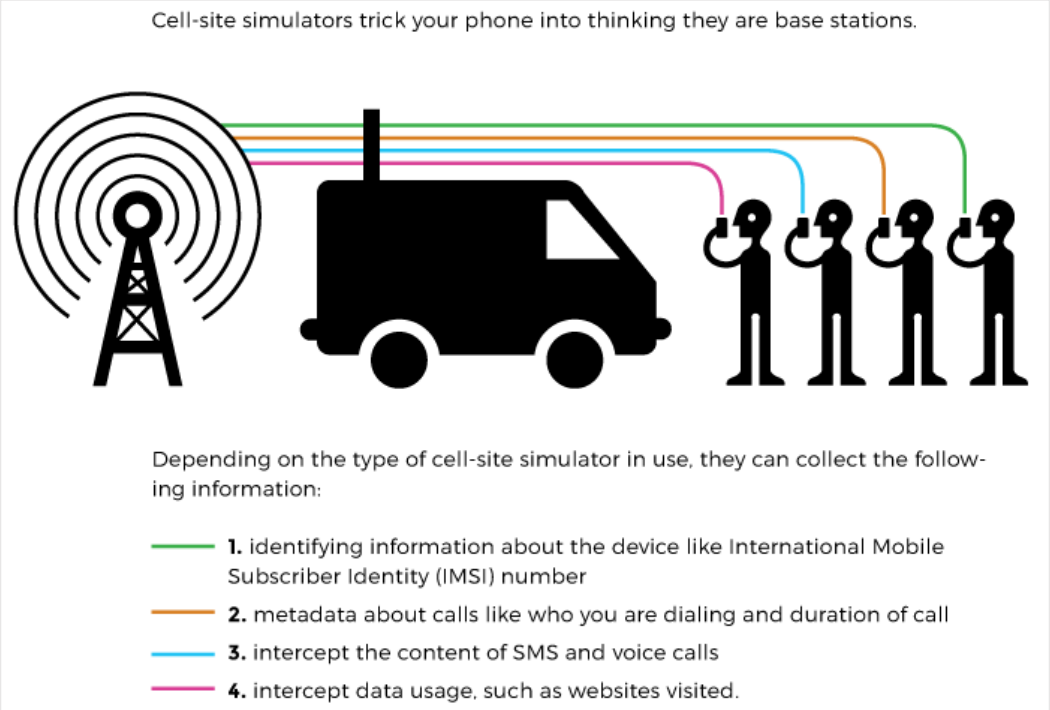
(Intentionally blank.)

[2] STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 114TH CONG., LAW ENFORCEMENT USE OF CELL-SITE SIMULATION TECHNOLOGIES: PRIVACY CONCERNS AND RECOMMENDATIONS 36 (2016) [hereinafter HOUSE OVERSIGHT REPORT ON CELL-SITE SIMULATORS].

[3] This explanation is intentionally simplified—it does not delve into the differences between a cellular antenna, a cellular tower, a cell site, and a coverage cell, nor does it cover the backend architecture of wireless networks. Those engineering details are, in my view, not essential to understanding cell-site simulators and the other cybersecurity risks that I describe in this testimony. I would be glad to provide additional detail as the Subcommittee finds valuable.

[4] The term "IMSI catcher" describes how cell-site simulators are able to identify the unique serial number on a mobile device's SIM card, the International Mobile Subscriber Identity (IMSI), by attracting ("catching") the device. Cell-site simulators are often referred to as "Stingrays" because one of the most popular models for law enforcement usage is the Harris Corporation Stingray. Some reports on cell-site simulators use the colloquial term "Dirtbox," because another popular law enforcement model is the Digital Receiver Technology DRTBox.

Figure: Diagram of how cell-site simulators operate.[5]



The most serious cell-site simulator risks are associated with second-generation ("2G") wireless protocols, which were initially deployed in the 1990s and remain operational today to support legacy devices.[6] The 2G wireless protocols do not include authentication for cellular towers. As a result, 2G cell-site simulators can fully mimic a cellular tower and have complete control over a mobile device's connectivity. These cell-site simulators can identify and track nearby mobile devices, and can intercept or block voice, text, and data communications involving those devices.

While more recent 3G and 4G wireless protocols include authentication for cellular towers, they still have significant cell-site simulator vulnerabilities.

One class of attack relies on downgrading the connection to 2G, such as by sending an instruction to a mobile device to disconnect from 3G and 4G, or by jamming the radio spectrum used for 3G and 4G connectivity.[7]

---

[5] Elec. Frontier Found., Cell-Site Simulators / IMSI Catchers, https://www.eff.org/pages/cell-site-simulatorsimsi-catchers (2017).

[6] *See* Kristin Paget, *Practical Cellphone Spying*, DEF CON 18 (July 31, 2010), https://www.youtube.com/watch?v=fQSu9cBaojc (demonstrating a homemade 2G cell-site simulator).

[7] DEP'T OF HOMELAND SEC., STUDY ON MOBILE DEVICE SECURITY 47-48 (2017) [hereinafter DHS MOBILE DEVICE SECURITY STUDY] (describing downgrade attacks); NAT'L INST. FOR STANDARDS & TECH., SPECIAL PUB. 800-187, GUIDE TO LTE SECURITY 31 (2017) [hereinafter NIST LTE SECURITY GUIDE] (same); Altaf Shaik et al., *Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems*, PROC. NETWORK & DISTRIBUTED SYSTEMS SECURITY SYMP., Feb. 2016, at 10 (detailing a downgrade attack against 4G LTE networks); Roger Piqueras Jover, Bloomberg LP, *LTE Security, Protocol Exploits, and Location Tracking Experimentation with Low-Cost Software Radio* (manuscript at 6-7), https://arxiv.org/pdf/1607.05171.pdf (same).

Another type of attack on 3G and 4G networks exploits unauthenticated network configuration instructions.[8] Researchers have shown that these commands can be used to identify nearby mobile devices and precisely track the location of a target mobile device.

A third class of attack on 3G and 4G wireless networks takes advantage of femtocells, consumer hardware sold by wireless providers that extends coverage indoors and in rural areas.[9] Researchers have demonstrated that it is possible to convert a femtocell into a cell-site simulator and intercept calls, text messages, and data from nearby mobile devices.

A fourth type of attack involves tricking a wireless carrier into trusting the cell-site simulator as if it were a roaming network partner.[10] The operator of a 3G or 4G cell-site simulator could induce the wireless carrier to assist with authenticating itself, then successfully mimic a roaming cellular tower. This class of attack would allow for eavesdropping and location tracking.

These types of cell-site simulator risks are, to be sure, not exhaustive. Researchers continue to identify new flaws in 3G and 4G protocols and how those protocols have been implemented. At minimum, it is certain that 3G and 4G networks remain vulnerable to cell-site simulators. It is also certain that, because wireless protocols remain deployed for decades, cell-site simulators pose a long-term cybersecurity risk.

Cell-site simulators vary substantially in their cost, range, form factor, and capabilities. Researchers have demonstrated proof-of-concept devices that consist of a laptop and small radio accessories, cost thousands of dollars, and can cover a large indoor space.[11] Cell-site simulators marketed to law enforcement agencies are most commonly sold in a vehicle mounted configuration, but are also available in portable and aircraft mounted form factors.[12] These devices cost between tens of thousands and hundreds of thousands of dollars, and usually have a

[8] Shaik, *supra* note 7, at 5-9 (describing several location tracking attacks against 4G LTE networks, including precise location tracking attacks that use a cell-site simulator); Jover, *supra* note 7, at 5, 7-8 (same); Stig F. Mjølsnes & Ruxandra F. Olimid, *Easy 4G/LTE IMSI Catchers for Non-Programmers* (manuscript at 7-9), https://arxiv.org/pdf/1702.04434.pdf (providing a step-by-step tutorial for a 4G LTE cell-site simulator).
[9] *See* Doug DePerry et al., *Traffic Interception & Remote Mobile Phone Cloning with a Compromised CDMA Femtocell*, BLACK HAT USA (July 31, 2013), https://www.youtube.com/watch?v=WGxF1N3RESQ (describing a proof-of-concept femtocell attack and reviewing prior work); DHS MOBILE DEVICE SECURITY STUDY, *supra* note 7, at 52 (summarizing femtocell attacks and collecting prior work); NIST LTE SECURITY GUIDE, *supra* note 7, at 32 (summarizing femtocell attacks).
[10] Karsten Nohl, *Mobile Self-Defense*, CCC (Dec. 27, 2014), https://www.youtube.com/watch?v=nRdJ0vaQt0o (describing this class of attack).
[11] *See supra* notes 6-9.
[12] *See* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J., Nov. 13, 2014 (describing how the U.S. Marshals Service operates airborne cell-site simulators); Curtis Waldman, *Here's How Much a StingRay Cell Phone Surveillance Tool Costs*, MOTHERBOARD (Dec. 8, 2016), https://motherboard.vice.com/en_us/article/gv5k3x/heres-how-much-a-stingray-cell-phone-surveillance-tool-costs (providing a price list of Harris Corporation cell-site simulator equipment available for sale to law enforcement).

range of approximately a thousand feet.[13] Illegal cell-site simulators are readily available on the black market.[14]

Detecting a cell-site simulator is exceedingly difficult. The usual approach is to examine nearby cellular towers for unusual attributes.[15] There are both free and commercial tools that attempt to detect cell-site simulators in this way, including the technology that the Department of Homeland Security used in its 2017 test deployment.[16]

The challenge with detecting cell-site simulators is that legitimate cellular towers can be configured with unusual settings, or can be inadvertently misconfigured, or might operate on a temporary basis (e.g. for a special event). Automated tools provide a hint about possible cell-site simulator operation, but immediate investigative follow-up is required to confirm. To my knowledge, other than the recent DHS pilot project, no component of the United States Government has acknowledged a capability to detect cell-site simulators in the field, no wireless carrier has acknowledged such a capability, and the Department of Justice has not initiated any prosecution for operating a cell-site simulator.[17]

While cell-site simulators have understandably captured the public imagination owing to their unusual design, surreptitious nature, and use by law enforcement agencies, there are other significant cybersecurity vulnerabilities in the nation's wireless infrastructure that merit congressional scrutiny. I would like to call the Subcommittee's attention to three other areas of communications cybersecurity where improvements are necessary and overdue.

---

[13] *Examining Law Enforcement Use of Cell Phone Tracking Devices: Hearing Before the Subcomm. on Info. Tech. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 12 (2015) (statement Seth Stodder, Assistant Sec'y, Threat Prevention & Sec. Policy, Dep't of Homeland Sec.); Waldman, *supra* note 12.

[14] Ben Bryant, *The Black Market Dealers Selling Tactical Surveillance Equipment Online*, MOTHERBOARD (Jan. 15, 2016), https://motherboard.vice.com/en_us/article/wnx57m/the-black-market-dealers-selling-state-surveillance-equipment-online.

[15] *E.g.*, Peter Ney et al., *SeaGlass: Enabling City-Wide IMSI-Catcher Detection*, PROC. ON PRIVACY ENHANCING TECH'S, July 2017 (describing inconclusive efforts to detect cell-site simulators in Seattle and Milwaukee); Robyn Greene et al., *An OTI Experiment: Open Source Surveillance Detection*, NEW AMERICA (July 25, 2017), https://www.newamerica.org/oti/blog/oti-experiment-open-source-surveillance-detection/ (describing inconclusive efforts to detect cell-site simulators in Washington, DC); SnoopSnitch, https://opensource.srlabs.de/projects/snoopsnitch (free and open-source Android app for detecting suspicious cellular towers).

[16] Letter from Christopher C. Krebs, Senior Official Performing the Duties of the Under Sec'y, Nat'l Prot. & Programs Directorate, Dep't of Homeland Sec., to Sen. Ron Wyden (Mar. 26, 2018) (describing the DHS pilot program and noting that DHS does not currently possess the technical capability to detect cell-site simulators); Letter from Christopher C. Krebs, Senior Official Performing the Duties of the Under Sec'y, Nat'l Prot. & Programs Directorate, Dep't of Homeland Sec., to Sen. Ron Wyden (May 22, 2018) (similar).

[17] *Examining Law Enforcement Use of Cell Phone Tracking Devices: Hearing Before the Subcomm. on Info. Tech. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 33 (2015) (responses of Elana Tyrangiel, Principal Deputy Assistant Att'y Gen., Dep't of Justice) (suggesting that DOJ is not aware of any unlawful cell-site simulator operation); *id.* at 46 (responses of Seth Stodder, Assistant Sec'y, Threat Prevention & Sec. Policy, Dep't of Homeland Sec.) (affirming that DHS is not aware of any unlawful cell-site simulator operation).

B. SS7 and Diameter

Signaling System 7 (SS7) and Diameter are the protocols that wireless carriers use to exchange information about mobile devices and route calls and text messages when a mobile device is roaming. When you bring your smartphone overseas, for example, SS7 and Diameter enable you to use a foreign wireless carrier while billing your domestic wireless carrier.

Like the 2G cellular protocols, SS7 and Diameter were designed without adequate authentication safeguards.[18] As a result, attackers can mimic legitimate roaming activity to intercept calls and text messages, and can imitate requests from a carrier to locate a mobile device. Unlike cell-site simulator attacks, SS7 and Diameter attacks do not require any physical proximity to a victim.

There are defenses available against these attacks, such as firewalls that reject untrustworthy SS7 and Diameter messages and network monitoring systems that identify suspicious patterns of activity. It is unclear how widely deployed and how effective these defenses are on the nation's communications infrastructure. In its 2017 study of mobile device security, DHS expressed concern that "U.S. carriers have acknowledged . . . that SS7 and Diameter vulnerabilities potentially exist in their networks, but they have not quantified or characterized the extent or nature of these risks to their network."[19] DHS ultimately concluded that it "believes that all U.S. carriers are vulnerable" to SS7 and Diameter attacks.[20]

C. Mobile Device Security Updates

Mobile devices are essentially small computers, and like ordinary computers, their software contains security flaws. The companies that develop mobile operating systems, such as Google and Apple, regularly identify and issue updates to address these vulnerabilities. Maintaining an up-to-date device is essential because once a serious security vulnerability is disclosed, there is often little time before criminals and foreign adversaries attempt to exploit the vulnerability.

Unfortunately, many mobile devices do not receive timely software security updates, leaving users at significant risk.[21] This problem is especially acute in the Android ecosystem, where critical security updates can be delayed by months and sometimes are never made available. The cause of these update deficiencies is the interplay between operating system vendors, device manufacturers, and wireless carriers, who must all approve a security update before it reaches a mobile device.

---

[18] DHS MOBILE DEVICE SECURITY STUDY, *supra* note 7, at 53, 76-77 (describing attacks against SS7 and Diameter). These cybersecurity vulnerabilities are not new; weaknesses in SS7 were identified 20 years ago, but have remained inadequately addressed. Joseph Cox, *Telecoms Knew About Spying Loophole for Decades, Did Nothing*, DAILY BEAST (Sept. 1, 2017), https://www.thedailybeast.com/telecoms-knew-about-spying-loophole-for-decades-did-nothing.

[19] DHS MOBILE DEVICE SECURITY STUDY, *supra* note 7, at 91.

[20] *Id.* at 77.

[21] *See* FED. TRADE COMM'N, MOBILE SECURITY UPDATES: UNDERSTANDING THE ISSUES (2018) (providing detailed quantitative data on the mobile device security update problem).

D. Caller ID

The caller ID system, at present, depends on trusting a caller; there is no means of reliably authenticating the caller's number. As a result, criminals can easily spoof legitimate telephone numbers to harass Americans and perpetrate frauds.

In just this month, Americans will receive billions of unlawful automated telephone calls.[22] These "robocall" schemes take advantage of our unreliable caller ID system to generate a large number of automated calls from numbers that appear trustworthy, such as numbers that share an area code and prefix. The calls often originate outside the United States and outside the reach of law enforcement, and Americans can do relatively little to protect themselves.

The long-term fix for caller ID and robocalls is rigorous authentication in our telephone networks.[23] In 2016, the major wireless carriers committed to targeting rollout for caller ID authentication in the first quarter of 2018.[24] As of today, though, not one major wireless carrier has adopted rigorous caller ID authentication—and at least three of the carriers charge a monthly fee for anti-robocall services.

II. Criminal and Foreign Government Use of Cell-Site Simulators

The possible criminal uses of cell-site simulators are limited only by our collective imagination. For example, by intercepting wireless communications, criminals could capture private financial information and steal funds; they could collect sensitive medical information and conduct blackmail; or they could obtain confidential business information for commercial gain. These are not hypotheticals; the Department of Justice routinely prosecutes individuals who have misappropriated and misused private communications (albeit via other technical means).

Cell-site simulators also pose a serious national security threat. The federal government is the nation's largest consumer of commercial wireless services, and it is susceptible to the same cybersecurity risks in our communications infrastructure. A foreign intelligence service could easily use cell-site simulators to collect highly confidential information about government operations, deliberations, and employee movements. And, while I have no reason to believe that cell-site simulators could compromise classified federal data, a foreign intelligence service may be able to use these devices to deny mobile access to classified networks and track the location of devices that handle classified material.[25]

The other serious cybersecurity vulnerabilities that I highlighted above—SS7 and Diameter, mobile device security updates, and caller ID—also pose significant criminal and national security risks.

---

[22] Tara Siegel Bernard, *Yes, It's Bad. Robocalls, and Their Scams, Are Surging.*, N.Y. TIMES, May 6, 2018.
[23] FED. COMMC'NS COMM'N, ROBOCALL STRIKE FORCE REPORT 4-9 (2016) (describing the role of caller authentication in combating robocalls).
[24] *Id.* at 7-8.
[25] *See* Defense Info. Systems Agency, *DOD Mobility Classified Capability - Secret*, https://www.disa.mil/Enterprise-Services/Mobility/DOD-Mobility/DMCC/Secret (describing how the Department of Defense uses commercial Android smartphones as a platform for handling Secret-level material).

Last year, for example, criminals used SS7 to intercept banking text messages directed to the subscribers of a European wireless carrier.[26] They were then able to loot victims' accounts. These vulnerabilities are so significant that the National Institute of Standards and Technology now cautions against using text messages for user authorization purposes.[27] At least one major wireless carrier in the United States has already experienced a data breach involving SS7.[28]

In 2015, ProPublica reported that Department of Defense smartphones—including smartphones that handle classified information—were not receiving prompt software security updates.[29] As a result, these smartphones remained vulnerable for months to critical and easily exploited vulnerabilities.

Congress has a number of tools at its disposal to address these pervasive cybersecurity problems in the nation's wireless infrastructure, including new regulation of the telecommunications sector. In my view, the most promising path forward—both because it could be immediately actionable and bipartisan—is to leverage the federal government's acquisitions.[30]

According to OMB, the United States Government spends about a billion dollars every year on cellular service and mobile devices.[31] And yet, as the Department of Homeland Security acknowledged in its April 2017 study on mobile device security, the federal government has little assurance that it is paying for cellular service and mobile devices that incorporate cybersecurity best practices.[32]

Congress should condition its substantial wireless outlays on implementation of appropriate cybersecurity safeguards. NIST, which is within this Committee's jurisdiction, could play a central role in developing, documenting, and updating those best practices—much like it already does in other areas of cybersecurity.

---

[26] Dan Goodin, *Thieves Drain 2FA-Protected Bank Accounts by Abusing SS7 Routing Protocol*, ARS TECHNICA (May 3, 2017), https://arstechnica.com/information-technology/2017/05/thieves-drain-2fa-protected-bank-accounts-by-abusing-ss7-routing-protocol/.

[27] Devin Coldewey, *NIST Declares the Age of SMS-Based 2-Factor Authentication Over*, TECHCRUNCH (July 25, 2016).

[28] Letter from Sen. Ron Wyden to Ajit Pai, Chairman, Fed. Commc'ns Comm'n (May 29, 2018) ("One of the major wireless carriers informed my office that it reported an SS7 breach . . . .").

[29] Jeff Larson, *Telecoms, Manufacturers Delaying Critical Patches for Classified Military Smartphones*, PROPUBLICA (Nov. 9, 2015), https://www.propublica.org/article/critical-patches-for-classified-military-smartphones-delayed.

[30] There has been increasing bipartisan interest in proposals to address cybersecurity risk by leveraging federal expenditures. This year's NDAA, for example, includes bipartisan provisions that would condition federal technology expenditures to mitigate supply chain risks. The FCC unanimously issued a proposal to address cybersecurity supply chain risks in commercial communications networks by conditioning its financial support for universal service. And, over in the Senate, a bipartisan group has proposed legislation that would condition federal technology purchases on implementation of cybersecurity best practices.

[31] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB MEMO. NO. M-16-20, IMPROVING THE ACQUISITION AND MANAGEMENT OF COMMON INFORMATION TECHNOLOGY: MOBILE DEVICES AND SERVICES 1 (2016).

[32] *See* DHS MOBILE DEVICE SECURITY STUDY, *supra* note 7, at 91-92 (explaining the DHS can only make cybersecurity risk assessments based on the information that wireless carriers elect to voluntarily provide).

At minimum, in my view, Congress should condition federal wireless expenditures on the following cybersecurity best practices.

- Wireless carriers should undergo regular cybersecurity audits, including to address the threats posed by cell-site simulators and SS7 and Diameter attacks. Carriers should commit to immediately remedying any identified issues.

- Operating system vendors and device manufacturers should implement defenses against 2G cell-site simulators. For example, smartphones could provide a security warning before connecting to a 2G cellular network (like they already do for insecure wi-fi networks), or they might provide an option to disable 2G connectivity (like they already do for roaming).[33]

- Carriers should deploy commercially available firewalls, filters, and network monitoring tools to address SS7 and Diameter threats.[34]

- Operating system vendors, device manufacturers, and wireless carriers should commit to maintaining mobile devices with prompt security updates for a defined period of time after sale. These stakeholders should also commit to providing clear notice in advance of discontinuing prompt security updates.

- Carriers should commit to a near-term rollout of authenticated caller ID, with a specific timeline for adoption.

III. Law Enforcement Use of Cell-Site Simulators

Federal, state, and local law enforcement agencies use cell-site simulators in the course of conducting criminal investigations. At present, the federal government owns over 400 cell-site simulators, and at least 73 state and local law enforcement agencies own cell-site simulators.[35]

Law enforcement cell-site simulators operate in one of two modes: they are either used to track the location of a suspect's mobile device, or they are used to identify all the mobile devices nearby (sometimes dubbed a "site survey").[36] Cell-site simulators can be particularly valuable when law enforcement officers are tracking a suspect indoors, where other mobile device location techniques may be much less precise.

---

[33] Some Android mobile devices already offer the latter option, but it is not easily accessible to users.

[34] *See* COMMC'NS SECURITY, RELIABILITY & INTEROPERABILITY COUNCIL V, WORKING GROUP 10: LEGACY SYSTEMS RISK REDUCTIONS (2017) (describing best practices for SS7 and Diameter security); GSMA, FS.11 (2015) (similar).

[35] HOUSE OVERSIGHT REPORT ON CELL-SITE SIMULATORS, *supra* note 2, at 13-14; ACLU, *Stingray Tracking Devices: Who's Got Them?* (Mar. 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them.

[36] While several of the cell-site simulators that are available to law enforcement agencies have the hardware capability to intercept communications, to my knowledge, no law enforcement agency has acknowledged using that capability and no cell-site simulator vendor has acknowledged enabling that capability on the equipment that it has sold. Both the Department of Justice and the Department of Homeland Security confirmed to the House Oversight Committee in 2015 that they do not use and do not plan to use cell-site simulators to intercept communications.

There are three distinct areas of federal law that regulate police use of cell-site simulators: the Fourth Amendment, the Electronic Communications Privacy Act, and the Communications Act.[37]

A. The Fourth Amendment

Applying the Fourth Amendment to cell-site simulators is not a straightforward task.[38] Multiple ambiguous and overlapping areas of law are potentially determinative, including the reasonable expectation of privacy standard,[39] the third-party doctrine,[40] the public movements doctrine,[41] the confidential informant doctrine,[42] the consent doctrine,[43] and the Supreme Court's recognition of heightened privacy protection in the home.[44] Last week's decision in *Carpenter v. United States* did not lend much clarity; it both expressly reserved how the Fourth Amendment applies to real-time location tracking (including cell-site simulators) and it continued a trend of increasing judicial sensitivity to intrusive technology and location privacy.[45]

While a full analysis of how the Fourth Amendment applies to cell-site simulators is beyond the scope of this prepared testimony, I would like to emphasize that every recent judicial decision is in agreement: <u>When a law enforcement agency operates a cell-site simulator, it conducts a Fourth Amendment search and must presumptively obtain a warrant.</u>[46]

Furthermore, as a matter of executive branch policy, the Department of Justice and the Department of Homeland Security already obtain warrants before operating cell-site simulators.[47] While the Department of Justice has emphasized that it is not formally conceding

---

[37] A number of states have now adopted statutes that regulate cell-site simulators or location privacy. HOUSE OVERSIGHT REPORT ON CELL-SITE SIMULATORS, *supra* note 2, at 30. In the interest of brevity, I focus on federal law.

[38] *See* United States v. Patrick, 842 F.3d 540, 543-45 (7th Cir. 2016) (describing possible Fourth Amendment perspectives on cell-site simulators); Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 600-01 n.103 (briefly reviewing Fourth Amendment law on cell-site simulators).

[39] Katz v. United States, 389 U.S. 347 (1967).

[40] Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

[41] United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983).

[42] United States v. White, 401 U.S. 745 (1971); Hoffa v. United States, 385 U.S. 293 (1966).

[43] Florida v. Jimeno, 500 U.S. 248 (1991).

[44] Kyllo v. United States, 533 U.S. 27 (2001).

[45] Carpenter v. United States, No. 16-402, 2018 WL 3073916, at *13 (U.S. June 22, 2018) ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval).").

[46] United States v. Ellis, No. 13-CR-00818 PJH, 2017 WL 3641867, at *1-7 (N.D. Cal. Aug. 24, 2017); United States v. Lambis, 197 F. Supp. 3d 606, 609-11, 614-16 (S.D.N.Y. 2016); People v. Gordon, 58 Misc. 3d 544, 549-51 (N.Y. Sup. Ct. 2017); Jones v. United States, 168 A.3d 703, 711-13 (D.C. 2017); State v. Andrews, 134 A.3d 324, 339-52 (Md. Ct. Spec. App. 2016).

[47] *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, U.S. DEP'T JUST. (Sept. 3, 2015), http://www.justice.gov/opa/file/767321/download; Memorandum from Alejandro N. Mayorkas, Deputy Sec'y of Homeland Sec., to Component Chiefs, Department Policy Regarding the Use of Cell-Site Simulator Technology (Oct. 19, 2015), http://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.

that the Fourth Amendment applies to cell-site simulators, it is—at minimum—clearly acquiescing to a warrant requirement for their operation.

B. The Electronic Communications Privacy Act

The second area of federal law that relates to cell-site simulators is the Electronic Communications Privacy Act of 1986 (ECPA), the statutory scheme that regulates communications surveillance by federal, state, local, and tribal law enforcement agencies. Applying ECPA to police cell-site simulators is straightforward: officers must obtain a pen register and trap and trace device ("pen/trap") order, a minor procedural hurdle that requires self-certification that operation of the cell-site simulator may produce evidence relevant to a criminal investigation.[48]

Because the Fourth Amendment likely requires a warrant, the provision of ECPA that authorizes pen/trap surveillance is likely unconstitutional as applied to cell-site simulators.[49] Under current law, officers are likely required to obtain a warrant (to satisfy the Fourth Amendment) in conjunction with a pen/trap order (to satisfy ECPA) before operating a cell-site simulator.

C. The Communications Act

The Communications Act of 1934 is the organic act for the Federal Communications Commission (FCC) and is the final area of federal law that regulates cell-site simulators. Importantly, the Communications Act does not regulate federal use of cell-site simulators; it only applies to cell-site simulators operated by state, local, and tribal law enforcement officers.[50]

The first component of the Communications Act that relates to cell-site simulators is Section 302, which authorizes the FCC to regulate the sale and marketing of wireless devices in order to prevent radio interference. Under its Section 302 authority, the FCC has developed an intricate regulatory framework and administrative process for equipment authorization.[51] Consistent with its rules and process, the FCC has elected to authorize several commercial cell-site simulators for marketing and sale within the United States, provided that the purchaser must be a law enforcement agency and must sign a nondisclosure agreement with the Federal Bureau of Investigation.[52] In my view, cell-site simulator vendors are clearly in compliance with Section 302 of the Communications Act and the FCC's implementing rules.

---

[48] Under the ECPA statutory definitions, operating a cell-site simulator constitutes use of a pen register and a trap and trace device because it involves collection of "dialing, routing, addressing, and signaling information." 18 U.S.C. §§ 3121, 3127. As a result, law enforcement investigators must obtain a pen/trap order. 18 U.S.C. §§ 3122-23.

[49] 18 U.S.C. § 3123.

[50] 47 U.S.C. §§ 302a(c) (exempting devices used by the federal government from the FCC's equipment authorization authority); 305(a) (exempting transmissions by the federal government from the FCC's spectrum authority).

[51] 47 C.F.R. §§ 2.801-.1207.

[52] HOUSE OVERSIGHT REPORT ON CELL-SITE SIMULATORS, *supra* note 2, at 31-32 (describing the FBI nondisclosure agreements associated with FCC equipment authorization).

The second component of the Communications Act that regulates cell-site simulators is Section 301, which provides that anyone making radio transmissions must be covered by an FCC authorization to transmit. In this area, too, the FCC has adopted intricate regulations and administrative procedures for granting licenses and authorizations, and for license transfer and leasing. In general, the Commission has divvied up radio spectrum by frequency band, geography, and power levels, and has designated some spectrum as exclusively licensed, some spectrum as shared, and some spectrum as unlicensed.

The key fact for law enforcement cell-site simulators is that cellular networks operate on exclusively licensed spectrum. The major wireless carriers have paid billions of dollars to the FCC to secure those reserved transmission rights. In order to function, though, law enforcement cell-site simulators must necessarily broadcast on that same licensed spectrum.

There is no provision in the FCC's rules that specially authorizes law enforcement agencies to transmit on licensed cellular spectrum.[53] There are also, to my knowledge, no spectrum leasing agreements between law enforcement agencies and wireless carriers that authorize cell-site simulator operation.[54]

As a result, it is currently a violation of Section 301 of the Communications Act for a state, local, or tribal law enforcement agency to operate a cell-site simulator. Police departments that operate cell-site simulators are susceptible to regulatory enforcement by the FCC and misdemeanor prosecution by the Department of Justice.[55]

I do not offer this legal analysis lightly. I believe that cell-site simulators are legitimate investigative tools, and that they should be available to law enforcement agencies when subject to appropriate procedural safeguards.[56] The nation's law enforcement professionals should not have to choose between on the one hand catching criminals with effective technology that they have lawfully purchased, and on the other hand risking regulatory or criminal liability. But, until Congress takes action, the nation's police departments will remain in legal limbo.[57] I encourage Congress to consider legislation that both resolves the Communications Act issues with cell-site simulators and codifies a warrant requirement for cell-site simulator operation.

---

[53] *See* Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, GN Docket No. 13-111, *Report and Order and Further Notice of Proposed Rulemaking*, at 9 (2017) (noting that a state correctional facility's deployment of technology equivalent to a cell-site simulator is unlawful without Commission approval and the consent of wireless carriers). The Commission has reserved a pool of wireless spectrum for public safety services, but the pool is not sufficient for cell-site simulator functionality. 47 C.F.R. §§ 90.15-22.

[54] *See* Fed. Commc'ns Comm'n, *Universal Licensing System - License Search*, http://wireless2.fcc.gov/UlsApp/UlsSearch/searchLicense.jsp (public database of spectrum licenses and leases).

[55] 47 U.S.C. §§ 501 (misdemeanor offense for statutory violations), 502 (monetary penalty for rule violations), 503-504 (administrative enforcement for statutory and rule violations).

[56] *See* Curtis Waltman, *Revisiting the Cell Site Simulator Census*, MUCKROCK (Dec. 4, 2017), https://www.muckrock.com/news/archives/2017/dec/04/revisiting-cell-site-simulator-census/ (presenting a cell-site simulator usage log from the Virginia State Police, who deployed the technology to locate murder suspects and fleeing fugitives).

[57] It is possible that the FCC could attempt to address this issue through its rulemaking authority, but it would likely require cooperation from the major wireless carriers because it would be effectively modifying their exclusive licenses.

The final component of the Communications Act that relates to cell-site simulators is Section 333, which prohibits willful interference with radio communications. In a 2015 enforcement action, the FCC unanimously interpreted this provision to cover not only radio jamming, but also disrupting communications by exploiting a wireless protocol vulnerability to disconnect a mobile device from a wireless network.[58] Depending on the technical details of law enforcement cell-site simulators, including whether they disrupt 911 calls and other connectivity, operating a cell-site simulator could also implicate Section 333's prohibition.[59]

* * *

Once again, thank you for the opportunity to address communications security and privacy at today's hearing. I look forward to your questions.

[58] In the Matter of M.C. Dean, Inc., E.B. File No. EB-SED-15-00018428, *Notice of Apparent Liability for Forfeiture*, 30 FCC Rcd. 13010, 13019-13024 (2015).

[59] *See* Colin Freeze, *RCMP Listening Device Capable of Knocking Out 911 Calls, Memo Reveals*, GLOBE & MAIL (Apr. 18, 2016), https://www.theglobeandmail.com/news/national/rcmp-listening-tool-capable-of-knocking-out-911-calls-memo-reveals/article29672075/ (describing how, when Canada's federal police force tested its cell-site simulators, it found that they routinely interfered with 911 calls).

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu