# BOLSTERING DATA PRIVACY AND MOBILE SECURITY: AN ASSESSMENT OF IMSI CATCHER THREATS

## HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JUNE 27, 2018

**Serial No. 115–68**

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
30–878PDF WASHINGTON : 2018

## COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
DANA ROHRABACHER, California
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
RANDY K. WEBER, Texas
STEPHEN KNIGHT, California
BRIAN BABIN, Texas
BARBARA COMSTOCK, Virginia
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana
GARY PALMER, Alabama
DANIEL WEBSTER, Florida
ANDY BIGGS, Arizona
ROGER W. MARSHALL, Kansas
NEAL P. DUNN, Florida
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
DEBBIE LESKO, Arizona
EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
SUZANNE BONAMICI, Oregon
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
DONALD S. BEYER, JR., Virginia
JACKY ROSEN, Nevada
CONOR LAMB, Pennsylvania
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
PAUL TONKO, New York
BILL FOSTER, Illinois
MARK TAKANO, California
COLLEEN HANABUSA, Hawaii
CHARLIE CRIST, Florida

---

### SUBCOMMITTEE ON OVERSIGHT

RALPH LEE ABRAHAM, LOUISIANA, *Chair*

BILL POSEY, Florida
THOMAS MASSIE, Kentucky
BARRY LOUDERMILK, Georgia
ROGER W. MARSHALL, Kansas
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
LAMAR S. SMITH, Texas
DONALD S. BEYER, JR., Virginia
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
EDDIE BERNICE JOHNSON, Texas

# CONTENTS

**June 27, 2018**

# BOLSTERING DATA PRIVACY AND MOBILE SECURITY: AN ASSESSMENT OF IMSI CATCHER THREATS

---

**WEDNESDAY, JUNE 27, 2018**

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
*Washington, D.C.*

The Subcommittee met, pursuant to call, at 2:17 p.m., in Room 2318 of the Rayburn House Office Building, Hon. Ralph Abraham [Chairman of the Subcommittee] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

# Congress of the United States

## House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

Subcommittee on Oversight

***Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats***

Wednesday, June 27, 2018
2:00 p.m.
2318 Rayburn House Office Building

Witnesses

**Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology

**Dr. T. Charles Clancy**, Director, Hume Center for National Security and Technology, Virginia Tech

**Dr. Jonathan Mayer**, Assistant Professor of Computer Science and Public Affairs, Princeton University

# U.S. HOUSE OF REPRESENTATIVES
# COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

## HEARING CHARTER

June 27, 2018

**TO:** Members, Subcommittee on Oversight

**FROM:** Majority Staff, Committee on Science, Space, and Technology

**SUBJECT:** Oversight Subcommittee hearing: *Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats*

---

The Subcommittee on Oversight will hold a hearing entitled *Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats* on Wednesday, June 27, 2018, at 2:00 p.m. in Room 2318 of the Rayburn House Office Building.

**Hearing Purpose:**

The purpose of this hearing is to examine and assess the threats to mobile security and user privacy presented by international mobile subscriber identity (IMSI) catchers and similar technology. IMSI catchers, known colloquially as "Stingrays", exploit cellular vulnerabilities by intercepting and collecting data and information transmitted to and from mobile devices. In the hands of malicious or nefarious actors, the technology can be leveraged to gain access to calls, texts, and other information sent to and from the mobile devices of unwitting Americans. Officials with DHS recently disclosed signs of sophisticated technology, including IMSI catchers, near sensitive facilities including the White House. The hearing will focus on the threats this technology poses to data security and privacy, as well as the steps industry and government can take to better mitigate such threats in the future.

**Witness List:**

- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Dr. T. Charles Clancy**, Director, Hume Center for National Security and Technology, Virginia Tech
- **Dr. Jonathan Mayer**, Assistant Professor of Computer Science and Public Affairs, Princeton University

**Staff Contact:**

For questions related to the hearing, please contact Tom Connally or Duncan Rankin of the Majority Staff at 202-225-6371.

Chairman ABRAHAM. The Subcommittee on Oversight will come to order. Without objection, the Chair is authorized to declare recesses of the Subcommittee at any time.

Good afternoon and welcome to today's hearing entitled "Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats."

I recognize myself for five minutes for an opening statement.

Good afternoon again. Welcome to today's Oversight Subcommittee hearing "Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats." The purpose of today's hearing is to examine the threats that IMSI catchers and other similar technologies pose to mobile security and user privacy.

IMSI catchers and rogue base stations, commonly known by their brand name "Stingray," are devices used for intercepting cellular traffic and data. Today we will hear from government and academic experts about the basics of the technology, the ways in which it can be used by both legitimate and illegitimate actors, and potential methods to mitigate the risks these devices pose.

Regrettably, although they were invited, the Department of Homeland Security, DHS, declined to provide a witness today and instead provided a briefing to Members and staff last week. While this was helpful in giving some context to the matter, it was no substitute for a public discussion on such a serious issue. It would have been substantially more helpful for DHS to have been present today, to be part of the dialogue, inform the American public, and answer questions about their work in this area. With that said, I would like to thank our witnesses for participating today and taking time out of their schedules to testify on this very important matter.

Historically, the use of IMSI catcher technology has been limited to law enforcement, Department of Defense, and intelligence services. This was due in large part to the high cost of acquiring the equipment. However, as sophisticated technologies have become more commonplace and advances in manufacturing have made the production of highly technical products easier and cheaper, IMSI catcher technology and nefarious actors looking to exploit it have been proliferated.

While awareness is important, it is simply not enough to acknowledge an issue that needs to be addressed. Instead, we must also gain an understanding of the technology—the nature of the technology, the complexity of the technology, and the disruptive ability like IMSI catchers challenge, and the challenges they present. This is a responsibility the Committee takes seriously, and one which the Committee has a long history of meeting through vigorous oversight of emerging forms of research and technology. I believe today's hearing will yet add another important chapter to that history.

As with much of technology in the modern age, IMSI catchers are a double-edged sword. On one hand, when used for legitimate law enforcement purposes, these technologies have the potential to positively impact society in a substantive and meaningful way. The ability to covertly track a suspect or intercept their data has the potential to help law enforcement coordinate safer arrests and cer-

tainly put more criminals behind bars, keeping our men and women in uniform, as well as our communities, safe.

However, as we have seen with many new technologies and law enforcement tools, striking the appropriate balance between safety and privacy is not always easy. Just this past week, the Supreme Court ruled in Carpenter v. United States that cell phone location records are protected under the Fourth Amendment, previously a legal grey area. While this ruling does not purport to apply to real-time data tracking, the type IMSI catcher technology could provide, it raises the question of what the appropriate balance is between protecting privacy and empowering law enforcement to do their job.

Similarly, we must consider what defenses we can and should employ to protect our privacy and national security. IMSI catcher technology is ripe for exploitation by foreign nations seeking to spy on American government officials and is likely already being used to do so. The cryptographic standards and methods used to protect U.S. government officials and important government information are something the National Institute of Standards and Technology is well positioned to produce, but this too creates a dilemma.

As we saw with the San Bernardino terrorist's iPhone, sophistication—sophisticated encryption meant to protect user data and privacy brings with it a set of different, but no less consequential, issues. In the case of IMSI catcher technologies, to what degree should the general public be able to shield themselves from being caught in a foreign intelligence operation? To what degree might techniques meant to shield data from prying eyes prevent law enforcement from doing their jobs? How much privacy should we trade for security at the civilian and governmental levels? These are fundamental questions that must be asked.

While I doubt we will hear an easy answer to these questions during today's hearing, we will hear informed perspectives from our witnesses on these and other important questions. It is my hope that we will leave here not only with a better understanding of this technology, but with forward-looking thoughts about possible answers to, and solutions for, these tough questions. Again, I want to thank our witnesses for agreeing to be here to highlight this important topic.

[The prepared statement of Chairman Abraham follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
June 27, 2018

Media Contacts: Heather Vaughan, Bridget Dunn
(202) 225-6371

## Statement by Chairman Ralph Abraham (R-La.)

*Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats*

**Chairman Abraham:** Good afternoon and welcome to today's Oversight Subcommittee hearing: "*Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats.*" The purpose of today's hearing is to examine the threats that IMSI catchers and other similar technologies pose to mobile security and user privacy.

IMSI catchers and rogue base stations—commonly known by their brand name "Stingray"—are devices used for intercepting cellular traffic and data. Today we will hear from government and academic experts about the basics of this technology, the ways in which it can be used by both legitimate and illegal actors, and potential methods to mitigate the risks these devices pose.

Regrettably, although they were invited, the Department of Homeland Security (DHS) declined to provide a witness today and instead provided a briefing to members and staff last week. While this was helpful in giving some context to this matter, it was no substitute for a public discussion on such a serious issue. It would have been substantially more helpful for DHS to have been present today, to be part of this dialogue, inform the American public, and answer questions about their work in this area. With that said, I would like to thank our witnesses for participating today and taking time out of their schedules to testify on this important matter.

Historically, the use of IMSI catcher technology has been limited to law enforcement, defense and intelligence services. This was due in large part the high cost of acquiring the equipment. However, as sophisticated technologies have become more commonplace and advances in manufacturing have made the production of highly technical products easier and cheaper, IMSI catcher technology and nefarious actors looking to exploit it have proliferated.

While awareness is important, it is simply not enough to acknowledge an issue needs to be addressed. Instead, we must also gain an understanding of the technological nature and complexity of disruptive technologies like IMSI catchers to alleviate the challenges they present. This is a responsibility the committee takes seriously, and one which the committee has a long history of meeting through vigorous oversight of emerging forms of research and technology. I believe today's hearing will add yet another important chapter to that history.

As with much of technology in the modern age, IMSI catchers are a double-edged sword. On the one hand, when used for legitimate law enforcement purposes, these technologies have the potential to positively impact society in a substantive and meaningful way. The

ability to covertly track a suspect or intercept their data has the potential to help law enforcement coordinate safer arrests and put more criminals behind bars, keeping our men and women in uniform, as well as our communities, safe.

However, as we have seen with many new technologies and law enforcement tools, striking the appropriate balance between safety and privacy is not always easy. Just this past week, the Supreme Court ruled in *Carpenter v. United States* that cell phone location records are protected under the Fourth Amendment, previously a legal grey area. While this ruling does not purport to apply to real-time data tracking—the type IMSI catcher technology could provide—it raises the question of what the appropriate balance is between protecting privacy and empowering law enforcement to do their job.

Similarly, we must consider what defenses we can and should employ to protect our privacy and national security. IMSI catcher technology is ripe for exploitation by foreign nations seeking to spy on American government officials and is likely already being used to do so. The cryptographic standards and methods used to protect US government officials and important government information are something the National Institute of Standards and Technology is well positioned to produce, but this too creates a dilemma.

As we saw with the San Bernardino terrorist's iPhone, sophisticated encryption meant to protect user data and privacy brings with it a set of different, but no less consequential, issues. In the case of IMSI catcher technologies, to what degree should the general public be able to shield themselves from being caught in a foreign intelligence operation? To what degree might techniques meant to shield data from prying eyes prevent law enforcement from doing their jobs? How much privacy should we trade for security at the civilian and governmental levels? These are fundamental questions that must be asked.

While I doubt we will hear an easy answer to these questions during today's hearing, we will hear informed perspectives from our witnesses on these and other important questions. It is my hope that we will leave here not only with a better understanding of this technology, but with forward-looking thoughts about possible answers to, and solutions for, these tough questions. Again, I want to thank our witnesses for agreeing to be here to highlight this important topic.

###

Chairman ABRAHAM. At this time, I'd ask unanimous consent that we include in the record the letter—I've got it here—that was sent to the Subcommittee this morning by the Electronic Privacy Information Center, or EPIC. Although I'm not sure I agree with the entirety of their statement, we will include this letter in the record.

[The information appears in Appendix I]

Chairman ABRAHAM. I now recognize Ranking Member of the Full Committee, Ms. Johnson, for an opening statement.

Ms. JOHNSON. Thank you very much, Chairman Abraham.

Cell-site simulators, also known as Stingrays, or IMSI catchers, is a technology that can be used to locate cellular devices and possibly intercept voice calls, text messages, and data communications from the cellular device. It is a valuable tool for our law enforcement and intelligence communities.

It is also, undoubtedly, a technology used by foreign intelligence services operating here in the United States. Indeed, the genesis of today's hearing were recent press reports that a Department of Homeland Security pilot program found rogue cell sites throughout Washington, D.C., including near the White House, FBI headquarters, and the Pentagon.

It is clear that foreign intelligence agencies are seeking to use cell-site simulators to collect intelligence on federal officials. What are we as a government doing to counter this particular threat? Unfortunately, neither the Department of Homeland Security nor the Federal Bureau of Investigation is here today to help provide some answers to these questions.

It is also unfortunate that President Trump appears to be taking no safeguards to protect himself from these cyber threats, and the Science Committee has taken no steps to use our oversight authority to investigate the White House's lack of cybersecurity precautions that we expect all other federal agencies to follow. I reiterate that Mr. Beyer's call and his statement and request that we hold a hearing on this subject in the near future.

I am glad though to have our witness panel here today, who can provide us with advice on what Congress should be doing to protect federal officials and federal agencies from cell-site simulators that exploit our cybersecurity vulnerabilities, particularly those that impact our national security interests.

Cell-site simulator technology also has implications for the privacy of Americans, as a law enforcement operation utilizing a cell-site simulator could be gathering data from thousands of nearby innocent citizens. In Baltimore, for instance, police used this technology without obtaining a warrant thousands of times in violation of the Fourth Amendment of the U.S. Constitution regarding an unreasonable search. Last week, the U.S. Supreme Court weighed in on this issue requiring police to obtain a warrant to gather cell phone location data. However, their decision did not specifically apply to cell-site simulators. So, it is unclear how these key privacy issues will be addressed by law enforcement agencies in the future.

I am glad Dr. Jonathan Mayer from Princeton University—a lawyer and a computer scientist—is here today. He is uniquely qualified to speak on these important privacy issues, as well as the wider implications of this technology and the dangers it poses to

our national security and our privacy. I look forward to hearing from him and other witnesses about how we can protect our national security and the privacy of our citizenry from attack by these rogue cell sites and other cyber threats that can target our mobile devices.

Thank you, Chairman Abraham, and thanks all of our witnesses for being here.

[The prepared statement of Ms. Johnson follows:]

OPENING STATEMENT
**Ranking Member Eddie Bernice Johnson (D-TX)**

House Committee on Science, Space, and Technology
Subcommittee on Oversight
*"Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats."*
June 27, 2018

Thank you Chairman Abraham.

Cell-site simulators, also known as Stingrays, or IMSI catchers, is a technology that can be used to locate cellular devices and possibly intercept voice calls, text messages, and data communications from the cellular device. It is a valuable tool for our law enforcement and intelligence communities.

It is also, undoubtedly, a technology used by foreign intelligence services operating here in the United States. Indeed, the genesis of today's hearing were recent press reports that a Department of Homeland Security (DHS) pilot program found rogue cell sites throughout Washington, D.C., including near the White House, FBI headquarters, and the Pentagon.

It is clear that foreign intelligence agencies are seeking to use cell site simulators to collect intelligence on federal officials. What are we as a government doing to counter this particular threat? Unfortunately, neither the Department of Homeland Security (DHS) nor the Federal Bureau of Investigation (FBI) is here today to help provide some answers to that question.

It is also unfortunate, as my colleague Mr. Beyer has pointed out, that President Trump appears to be taking no safeguards to protect himself from these cyber threats, and the Science Committee has taken no steps to use our oversight authority to investigate the White House's lack of cybersecurity precautions that we expect all other federal agencies to follow. I reiterate Mr. Beyer's call and request that we hold a hearing on this subject in the near future.

I am glad though to have our witness panel here today, who can provide us with advice on what Congress should be doing to protect federal officials and federal agencies from cell site simulators that exploit our cybersecurity vulnerabilities, particularly those that impact our national security interests.

Cell-site simulator technology also has implications for the privacy of Americans, as a law enforcement operation utilizing a cell site simulator could be gathering data from thousands of nearby innocent citizens. In Baltimore, for instance, police used this technology without obtaining a warrant thousands of times in violation of the Fourth Amendment to the U.S. Constitution regarding an unreasonable search. Last week, the U.S. Supreme Court weighed in on this issue requiring police to obtain a warrant to gather cell phone location data. However, their decision did not specifically apply to cell site simulators. So, it is unclear how these key privacy issues will be addressed by law enforcement agencies in the future.

I am glad Dr. Jonathan Mayer from Princeton University—a lawyer and a computer scientist — is here today. He is uniquely qualified to speak on these important privacy issues, as well as the wider implications of this technology and the dangers it poses to our national security and our privacy. I look forward to hearing from him and our other witnesses about how we can protect our national security and the privacy of our citizenry from attack by these rogue cell sites and other cyber-threats that can target our mobile devices.

Thank you Chairman Abraham and thank you to all of our witnesses for being here today

I yield back.

Chairman ABRAHAM. Thank you, Ms. Johnson.

I now recognize the Ranking Member of the Oversight Subcommittee, the gentleman from Virginia, Mr. Beyer, for an opening statement.

Mr. BEYER. Thank you, Chairman Abraham, very much, and thank you for your initiative to create this hearing.

Cell-site simulators, or IMSI catchers, pose risks to both our national security and our personal privacy. These devices are about the size of a laptop computer and can be placed in a van, hotel room, drone aircraft, or operated by someone sitting on a park bench. These rouge cell stations masquerade as legitimate cell towers and gather the data of cell phones in their proximity. They are powerful tools employed by both friendly and hostile intelligence agencies, criminals and others. They also play an important role in the operations of U.S. law enforcement and the U.S. intelligence community. However, U.S. law enforcement agencies have not always obtained appropriate authorization from the courts before they have employed these tools against suspected criminals, and this has led to improper incursions into the private lives of hundreds of American citizens.

Last week, the Supreme Court ruled that the government must now obtain a warrant when collecting cell phone data in certain cases. The court found, and I quote, "A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. Accordingly, when the government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." However, the court added that it was a narrow ruling, specifically stating, "We do not express a view on matters not before us: real-time CSLI, Cell-Site Location Information, or tower dumps." Unfortunately, it seems the constitutionality of cell-site simulator use by law enforcement agencies without a warrant remains unsettled.

Rogue cell-site simulators have not only affected our privacy, but they have endangered our national security. Last year, a Department of Homeland Security pilot project identified several rogue cell-site simulators near the White House and Pentagon, raising the specter of foreign intelligence agencies using IMSI catchers to target senior U.S. government officials right here in our Nation's Capital.

Ironically, at the same time we are holding an oversight hearing on the threat to mobile security of these sorts of rogue cell sites, President Trump continues to ignore basic cybersecurity practices. This has created a threat not only to his own personal privacy but also to our national security. A headline from a CNN story in April read, "Trump ramps up personal cell phone use." In May, POLITICO summed up the President's attitude towards the cybersecurity issues we're discussing today. The headline read "Too Inconvenient—Trump Goes Rogue on Phone Security." And making matters worse, President Trump recently said that he provided his direct phone number to North Korean dictator Kim Jong-un. Doing this has opened up an additional threat known as a Signaling System Seven, or SS7, attack that may permit access to President Trump's personal cell phone remotely by North Korean intelligence

operatives. Earlier this month, WIRED magazine published a story with the headline "Trump Says He Gave Kim Jong-un His Direct Number. Never Do That."

I am attaching all three articles to my statement.

Ongoing use of a reportedly unsecure cell phone by the President of the United States raises serious cybersecurity issues that this Committee should be examining. The Majority's Oversight Plan said the Science Committee would investigate cybersecurity incidents and compliance with "federal information security standards and guidelines" "regardless of where they may be found." Let me repeat, quote, "regardless of where they may be found." I wrote to Chairman Smith with Ranking Member Johnson and Mr. Lipinski in February of this year pointing out numerous cybersecurity practices of serious concern at the White House that warranted investigation. Unfortunately, we have not yet seen efforts by this Committee to uphold its oversight responsibilities to the American public and investigate these issues.

My good friend Chairman Abraham, I am asking you again, let's look at holding this hearing and investigating the potential threat by holding—by rogue cell-site simulators, but while we do this, we can't ignore the specific threats within blocks of the White House and President Trump's own failure to abide by cybersecurity best practices.

You know, In January 2018, the White House Chief of Staff Kelly banned the use of personal cell phones in the West Wing by White House employees. Yet, multiple media stories have continued to report that the President refuses to give up his personal cell phone or take proper cybersecurity measures to help identify and diminish cybersecurity threats. The President should not be held to a different standard than the rest of the federal government and our Committee should help the Executive Branch protect Mr. Trump from foreign adversaries, even if the President won't.

So I look forward to hearing from all of our witnesses today who help us explore ways to enhance our cybersecurity. It is unfortunate we don't have anyone from DHS or the telecommunications, but I hope we will be able to hear from them in the future. Successfully addressing these issues is going to take a collective effort and a continued commitment from a wide range of stakeholders.

Thank you, Chairman Abraham, and I yield back.

[The prepared statement of Mr. Beyer follows:]

OPENING STATEMENT
**Ranking Member Don Beyer (D-VA)**
**of the Subcommittee on Oversight**

House Committee on Science, Space, and Technology
Subcommittee on Oversight
*"Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats."*
June 27, 2018

Thank you, Chairman Abraham.

Cell site simulators or IMSI catchers, pose risks to both our national security and our personal privacy. These devices are about the size of a laptop computer and can be placed in a van, hotel room, drone aircraft, or operated by someone sitting on a park bench. These rouge cell stations masquerade as legitimate cell towers and gather the data of cell phones in their proximity. They are powerful tools employed by both friendly and hostile intelligence agencies, criminals and others. They also play an important role in the operations of U.S. law enforcement and the U.S. intelligence community. However, U.S. law enforcement agencies have not always obtained appropriate authorization from the courts before they have employed these tools against suspected criminals. This has led to improper incursions into the private lives of hundreds of American citizens.

Last week, the Supreme Court ruled that the government must now obtain a warrant when collecting cell phone data in certain cases. The court found, and I quote – "A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user," unquote. However, the court added that it was a narrow ruling, specifically stating, "We do not express a view on matters not before us: real-time CSLI [Cell-Site Location Information] or 'tower dumps." Unfortunately, it seems the constitutionality of cell site simulator use by law enforcement agencies without a warrant remains unsettled.

Rogue cell site simulators have not only affected our privacy, but they have endangered our national security. Last year, a Department of Homeland Security (DHS) pilot project identified several rogue cell site simulators near the White House and Pentagon—raising the specter of foreign intelligence agencies using IMSI catchers to target senior U.S. government officials here in our Nation's Capital.

Ironically, at the same time, we are holding an oversight hearing on the threat to mobile security of these sorts of rogue cell sites, President Trump continues to ignore basic cybersecurity practices. This has created a threat not just to his own personal privacy but also to our national security. A headline from a *CNN* story in April read, **"Trump ramps up personal cell phone use."** In May, *POLITICO* summed up the President's attitude towards the cybersecurity issues we are discussing today and the security precautions that should be taken to counter these threats.

The headline read: ***"'Too inconvenient': Trump goes rogue on phone security.'"*** Making matters worse, President Trump recently said that he provided his direct phone number to North Korean dictator Kim Jong-un. Doing this has opened up an additional threat known as a Signaling System Seven or SS7 attack that may permit access to President Trump's personal cell phone remotely by North Korean intelligence operatives. Earlier this month, *WIRED* magazine published a story with the headline: ***"Trump Says He Gave Kim Jong Un His Direct Number. Never Do That."***

I am attaching all three articles to my statement.

Ongoing use of a reportedly unsecure cell phone by the President of the United States raises serious cybersecurity issues that this Committee should be examining. The Majority's Oversight Plan for the 115th Congress said the Science Committee would investigate cybersecurity incidents and compliance with "federal information security standards and guidelines" *"regardless of where they may be found."* Let me repeat, quote: *"regardless of where they may be found."* I wrote to Chairman Smith with Ranking Member Johnson and Mr. Lipinski in February 2017 pointing out numerous cybersecurity practices of serious concern at the White House that warranted investigation. Unfortunately, we have seen no efforts by this Committee to uphold its oversight responsibilities to the American public and investigate these issues.

Chairman Abraham, holding this hearing and investigating the potential threat posed by rogue cell site simulators is a good idea. But I don't understand how we can investigate these issues and the specific threats that have been identified within blocks of the White House while ignoring the White House and President Trump's own failure to abide by cybersecurity best practices. In January 2018, the White House Chief of Staff banned the use of personal cell phone use in the West Wing by White House employees. Yet, multiple media stories have continued to report that the President refuses to give up his personal cell phone or take proper cybersecurity measures to help identify and diminish cybersecurity threats. The President should not be held to a different standard than the rest of the federal government and our Committee should help ensure the Executive Branch is taking appropriate cybersecurity measures to protect Mr. Trump from foreign adversaries, even if the President himself won't.

I look forward to hearing from all of our witnesses today who can help us explore ways to enhance our cybersecurity tools and plug our cybersecurity weaknesses. It is unfortunate that we do not have witnesses representing the Department of Homeland Security (DHS) or the telecommunications industry. I hope we are able to hear from them in the future. Successfully addressing these issues will take a collective effort and a continued commitment from a wide-range of stakeholders.

Thank you, Chairman Abraham. I yield back.

Chairman ABRAHAM. And now I will introduce our witnesses.

Our first witness is Dr. Charles H. Romine, director of the Information Technology Laboratory at NIST. Dr. Romine joined NIST in 2009 as an associate director for the program implementation. In November 2011, Dr. Romine became the director of Information Technology Laboratory at NIST. Dr. Romine received both his bachelor of arts degree in mathematics and his Ph.D. in applied mathematics from the University of Virginia. Welcome.

Dr. T. Charles Clancy, our next witness, he is the director of Virginia Tech's Hume Center for National Security and Technology. Dr. Clancy has worked with Virginia Tech since 2010 as a professor. Prior to that he worked at the National Security Agency from 2000 to 2010. He holds a bachelor's degree in computer engineering from Rose-Hulman Institute of Technology, and a master's degree in electrical engineering from the University of Illinois, Urbana-Champaign. Dr. Clancy also received a doctorate from the University of Maryland, College Park, in computer science.

Dr. Jonathan Mayer, our last witness, assistant professor at Princeton University's Department of Computer Science, and the Woodrow Wilson School of Public and International Affairs. Dr. Mayer previously worked for Senator Kamala Harris as a technology advisor in 2017. Prior to that he worked for the Federal Communications Commission Enforcement Bureau as a chief technologist from 2015 to 2017. He holds a bachelor's degree in public and international affairs from Princeton University. Dr. Mayer also received his juris doctorate and Ph.D. from Stanford University.

I now recognize Dr. Romine for five minutes to present his testimony.

## TESTIMONY OF DR. CHARLES H. ROMINE, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Dr. ROMINE. Chairman Abraham, Ranking Member Beyer, Ranking Member Johnson, and Members of the Subcommittee, I am Charles Romine, director of the Information Technology Laboratory at the National Institute of Standards and Technology, known as NIST. Thank you for the opportunity to appear before you today to discuss our role in mobile device security.

In the cybersecurity realm, NIST has worked with federal agencies, industry, and academia since 1972, and NIST's role has been expanded to research, develop, and deploy information security standards and technology to protect the federal government's information systems against threats, as well as to facilitate and support the development of voluntary industry-led cybersecurity standards and best practices for critical infrastructure.

Today, I'd like to talk about our work related to rogue base stations and the NIST Special Publication 800–187, Guide to LTE Security, released in December 2017.

Rogue base stations are unlicensed, cellular devices that are not owned or operated by a duly-licensed mobile network operator. They're known by many names, such as cell-site simulators, Stingrays, or International Mobile Subscriber Identity, or IMSI, catchers. Rogue base stations act as a cell tower and broadcast a signal pretending to be a legitimate mobile network that may trick an in-

dividual's device into connecting to it. The necessary hardware to build a rogue base station is inexpensive, easily obtained, and the software required is freely available.

Rogue base stations exploit the fact that mobile devices will connect to whichever base station is broadcasting as a device's preferred carrier network and is transmitting at the highest power level. Therefore, when a rogue base station is physically near a mobile device that is transmitting at higher power levels than the legitimate antenna, the device may attempt to connect to that malicious network.

The threats from rogue base stations can come from their performing a passive attack, known as IMSI catching. This attack collects mobile device identities without the user's knowledge. It poses a significant threat to user privacy and security and safety because a malicious actor can determine if a subscriber is in a given location at a given time. Unfortunately, IMSI catching is no longer an advanced or complex attack only accessible to a small number of individuals.

A more advanced attack that can be executed using a rogue base station is a type of man in the middle attack in which a malicious actor can force a user to downgrade to an older and less secure mobile network technology, such as 2G or 3G, that exposes that user to less robust security protections that exist in older versions of mobile networks, tricking the device into connecting to the rogue base station.

A complex denial of service attack can occur when a mobile device first connects to a network when certain messages can be sent to a device by a rogue base station, essentially fooling the device to into the equivalent of airplane mode. This can cause a denial of service that may persist until a hard reboot is done.

Since 2012, NIST has been working in cybersecurity aspect of telecommunications, focusing on 4G LTE networks used by public safety. This work enabled NIST to develop the guide to LTE security, which serves as a guide to the fundamentals of how LTE networks operate. It explores the LTE security architecture, and it provides an analysis of the threats posed to LTE networks and supporting mitigations. The guide is intended to educate federal agencies and other organizations that rely on 4G LTE networks as part of their operational environment.

NIST has been an active participant in the working group of the Standards Development Organization responsible for security and privacy of 3G and 4G LTE, and recently, 5G. Active participation with the mobile network ecosystem developing security standards for future networks is an important way NIST works to address security vulnerabilities in mobile networks today.

Security standards for 5G are, in fact, seeking to address issues surrounding rogue base stations through the introduction of optional privacy functionality. Once this functionality standard is developed for future networks, its implementation by mobile network operators will have the potential to eliminate the threat of today's passive sniffing IMSI catchers. In addition, the use of the optional security settings and next generation 5G technologies will go a long way to mitigate the usage of rogue base station technology.

Much work still needs to be done to ensure secure deployments. NIST will continue its research and development in the security of telecommunications, the publication of guidelines and best practices, and our work with international standards bodies and technical committees.

Thank you for the opportunity to testify on NIST's work regarding telecommunications security, and I will be pleased to answer any questions you may have.

[The prepared statement of Dr. Romine follows:]

Testimony of

Charles H. Romine, Ph.D.

Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

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

*"Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats"*

June 27, 2018

**Introduction**

Chairman Abraham, Ranking Member Beyer, and members of the Subcommittee, I am Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in telecommunications security.

**The Role of NIST in Cybersecurity**

Cybersecurity is a key priority of this Administration, for NIST, and across the Department of Commerce. With programs focused on national priorities, from advanced manufacturing and the digital economy to precision metrology, quantum science, and biosciences, NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, starting with the development of the data encryption standard, when the potential commercial benefit of this technology became clear. NIST's role, to research, develop, and deploy information security standards and technology to protect the federal government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347[1]) and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST guidelines are developed in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies and are frequently voluntarily used by other organizations, including small and medium-sized businesses, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, represent the state-of-art and have wide acceptance. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

As the principal advisor to the White House on information and communications policy, the Commerce's National Telecommunications and Information Administration (NTIA), collaborates with NIST to ensure that the equities of innovation, economic growth, and an open Internet are factored into cybersecurity policy decisions within both domestic and international fora.

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347; 116 Stat. 2899).

**Rogue Base Stations**

***Overview***

As explained in NIST Special Publication 800-187, "Guide to LTE Security," which I will discuss later in more detail, rogue base stations are unlicensed cellular devices that are not owned and operated by a duly-licensed mobile network operator. These devices broadcast on spectrum licensed to legitimate mobile network operators. They are known by many names, such as *Cell-Site Simulators, Stingrays* or *International Mobile Subscriber Identity (IMSI) catchers*. As cell-site simulators are also an important tool for law enforcement, we note that our statement focuses on the unauthorized use of such technology by non-law enforcement actors. Rogue base stations act as a cell tower and broadcast a signal pretending to be a legitimate mobile network that may trick an individual's device into connecting to it. The necessary hardware to build a rogue base station can be inexpensively obtained using commercial off-the-shelf parts. The software required to operate a rogue base station is open source and freely available.

Rogue base stations exploit the fact that mobile devices will connect to whichever base station is broadcasting as a device's preferred carrier network and is transmitting at the highest power level. Therefore, when a rogue base station is physically near a mobile device that is transmitting at higher power levels than the legitimate antenna, the device may attempt to connect to the malicious network. Mobile devices and networks are engineered to be backwards compatible interoperating with older mobile networks, providing maximum coverage to subscribers. Rogue base station attacks can take advantage of this interoperability and exploit weaknesses in these older mobile networks. Many rogue base stations broadcast an older second generation (2G) mobile network type, also referred to as Global System for Mobile communications (GSM), that does not have the security protections needed in today's communication environment. Examples of 2G weaknesses include a lack of mutual authentication and the use of weak or broken cryptographic algorithms.

***Threats***

Rogue base stations can perform a passive attack known as IMSI catching. This attack sniffs cellular communication without the user's knowledge to collect mobile device identities that are sent in an unencrypted manner. I am using the term "mobile devices" here to refer to any device with a cellular connection, such as a cellphone, tablet, laptop, or mobile hotspot. In fourth generation (4G) Long-Term Evolution (LTE) networks, device identities are known as "IMSI," and correlate to a specific subscriber. This identifier can be used to indicate who owns a mobile device. When a device is physically close to a rogue base station that is masquerading as a legitimate network, the device sends a message to initiate an *attach*, or connection, to the network. This message contains the subscriber identifier IMSI and information about the device's security capabilities. It is important to understand that in 4G LTE, this message is sent unprotected, *before* security is established.

It is commonplace today for individuals to constantly wear or keep their mobile devices close by. If a rogue base station is operating near someone's home or workplace, the operator of the rogue network may be able to infer whether a specific individual is present or not. This poses a significant threat to user privacy, and potentially safety, because a malicious actor can determine if a subscriber is in a given location at a given time. Compounding this issue is the fact that

passive sniffing of IMSIs is no longer an advanced or complex attack only accessible to a small number of individuals.

A more advanced attack that can be executed using rogue base stations is a type of "man in the middle" attack, in which a malicious actor can force a user to downgrade to an older, less secure mobile network technology such as 2G or 3G. Normally, mobile networks and user devices support interworking with legacy mobile networks (2G/3G) in order to provide the highest level of connectivity to their subscribers. For example, if an area does not have 4G LTE coverage, but does have 2G or 3G coverage, a mobile device can still connect to the mobile network. This interworking with legacy networks provides a seamless connection to the user; however, it exposes that user to less robust security protections and vulnerabilities that exist in older versions of mobile networks. As a result, a malicious actor running a rogue base station would be able to trick an attached device into connecting and execute a man in the middle attack on the device.

While there are no significant, currently publicly known weaknesses in the cryptographic algorithms used to protect the confidentiality and integrity of the 3G communications, significant weaknesses are known to exist for the 2G cryptographic algorithms used to protect the confidentiality and integrity of the air interface. The air interface is the radio frequency (RF) connection between the mobile device's antenna and the base station's antenna. Examples of broken 2G cryptographic algorithms are A5/1 and A5/2. Depending on the algorithm negotiated when a device connects to a rogue base station, a cryptographically broken algorithm may be selected to protect the cellular traffic. This can lead to a loss of call and data confidentiality.

A complex "denial of service" attack can occur when a mobile device first connects to a network, a process which is known as the "attach procedure." During the attach procedure, certain messages can be sent to a device by a rogue base station before security parameters are negotiated with the bona fide network. One such unprotected message may prevent a mobile device from completing the attach procedure. In response to receiving this message, a mobile device will no longer attempt to attach to this, or other, LTE networks, essentially going into the equivalent of "airplane mode." Since this message is sent before the mobile device can authenticate the network, the mobile device is unable to distinguish the rogue base station from an authentic network. This can cause a denial of service that may persist until a hard reboot (that is, completely powering the device off and then restarting it) of the mobile device is performed. Certain mobile device cellular implementations will not automatically try to reconnect if such a message is received.

**NIST activities related to Rogue Base stations**

NIST began working in the cybersecurity aspects of telecommunications in 2012, focusing on 4G LTE networks used by public safety. Ultimately, these activities enabled NIST to develop *Special Publication 800-187: Guide to LTE Security*.[2] The Guide to LTE Security was released in December 2017. This publication starts with the premise that cellular technology plays an increasingly large role as the primary portal to the internet for a large segment of the nation's population. One of the main drivers making this possible is the deployment of 4G LTE cellular technologies. This publication serves as a guide to the fundamentals of how LTE networks

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf

operate; it explores the LTE security architecture; and it provides an analysis of the threats posed to LTE networks and supporting mitigations. The document covers many areas of interest to the Committee, and includes a description of cell site simulators or rogue base stations as unlicensed base stations that are not owned and operated by an authentic mobile network operator. This NIST Special Publication is intended to educate federal agencies and other organizations who rely on 4G LTE networks as part of their operational environment.

Since 2012, NIST has been an active participant in the Third Generation Partnership's (3GPP's) Service and Systems Aspects (SA) Working Group 3. This working group is the standards development organization responsible for security and privacy of 3G and 4G LTE, and is currently developing 5G. Active participation with the mobile network manufacturers and carriers in developing security standards for future networks is an important way in which NIST is working to address security vulnerabilities in mobile networks today.

Security standards for 5G are, in fact, seeking to address issues surrounding rogue base stations through the introduction of optional privacy functionality. Once this functionality standard is developed for future networks, its implementation by mobile network operators will have the potential to eliminate the threat of today's passive sniffing IMSI catchers.

**Concluding Observations**

When compared to previous mobile networks, the security capabilities provided by 4G LTE are markedly more robust. The additions of mutual authentication between the mobile network and the mobile device, alongside the use of publicly reviewed cryptographic algorithms with sufficiently large key sizes, are positive steps forward in improving the security of mobile networks. The enhanced key separation introduced into the 4G cryptographic key hierarchy and the mandatory integrity protection also help to raise the bar. Yet 4G systems have a number of optional capabilities that mobile network operators must choose to implement. The use of the optional security settings and next generation 5G technologies will go a long way to mitigate the usage of rogue base station technology. To that extent, NIST also collaborates with our sister agency NTIA to maintain and enable U.S. 5G activities. NTIA actively identifies and studies additional spectrum bands to make available for commercial uses; supporting national and international efforts to set standards and harmonize spectrum; and helping industry to overcome obstacles in deploying the network infrastructure needed for 5G to flourish. This is essential to keeping U.S. companies at the forefront of the innovation in the wireless industry.

5G is a new and exciting technology with the ability to positively impact nearly every facet of the technology space. Much work still needs to be done to understand this technology and ensure secure deployments. NIST will continue its research and development in the security of telecommunications. We will continue to learn from our research and continue to build collaborations with industry in the publication of guidelines and best practices. NIST is also continuing to work with international standards bodies and technical committees. This is truly an exciting time in the continuing expansion of telecommunications to benefit the lives of every American.

Thank you for the opportunity to testify on NIST's work regarding telecommunications security. I will be pleased to answer any questions you may have.

**Charles H. Romine**

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of seven research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of $150 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission, to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

**Education:**
Ph.D. in Applied Mathematics from the University of Virginia.
B.A. in Mathematics from the University of Virginia.

Chairman ABRAHAM. Thank you, Romine—Dr. Romine.

All right, I now recognize Dr. Clancy for five minutes to present his testimony.

**TESTIMONY OF DR. T. CHARLES CLANCY,**
**DIRECTOR, HUME CENTER FOR NATIONAL SECURITY AND TECHNOLOGY,**
**VIRGINIA TECH**

Dr. CLANCY. Chairman Abraham, Ranking Members Beyer and Johnson, Subcommittee Members, my name is Charles Clancy and I am a professor of electrical and computer engineering at Virginia Tech where I direct the Hume Center for National Security and Technology. My current research sits at the intersection of 5G wireless, the internet of things, cybersecurity, and artificial intelligence. Prior to joining Virginia Tech, I led a portfolio of wireless research and development programs at the National Security agency.

It is my distinct pleasure to address this Committee on topics of critical national importance.

Security of wireless infrastructure is critical. These devices, wireless base stations, and core network infrastructure are a key part of our critical infrastructure ecosystem. While each generation of cellular technology improves security and privacy, the backward compatibility challenge means that even if we deploy highly secure 5G networks, most phones can still connect to insecure 2G networks, even though many of the national carriers in the United States have already decommissioned their 2G infrastructure.

This mixture of old and new technologies means that insecurity will always be part of the cellular ecosystem. Combatting threats to wireless network infrastructure requires a risk management approach that constantly evaluates potential vulnerabilities, observes threats, engineers countermeasures, and communicates best practices.

Specifically with respect to IMSI catchers, as we've heard, IMSI catchers, also known as Stingrays, have come to symbolize a wide range of different cellular surveillance technologies. Rogue base stations, a particular class of surveillance technology, also known as a cell-site simulator, are devices that act like cell towers. 2G technology is particularly susceptible to these threats because authentication in 2G is weak and the encryption has been cracked. 2G rogue base stations are able to lure a phone into connecting, eliciting that phone's identity, also known as IMSI, prevent it from disconnecting, query the phone's precise GPS location, and in certain cases, intercept voice, data, and SMS content. 3G and 4G rogue base stations are less capable because the underlying standards are more secure; however, they are still able to elicit a phone's identity.

Earlier this year, 5G adopted a proposal known as IMSI encryption, which prevents 5G rogue base stations from successfully eliciting a phone's identity, which was seen generally as a very positive step forward.

Rogue base stations can be used for a variety of applications, but are most commonly associated with IMSI catching. They interact with a phone for a few milliseconds to learn the phone's identity, and then pass that phone back to the real network.

Another class of device is a more generic cell phone interception system. These devices are purely passive. They don't transmit anything. They don't pretend to be a cell tower. However, particularly for 2G standards, which have been cracked, they are able to intercept in bulk voice, SMS, and data traffic that is traversing those networks. For 3G and 4G networks that are protected by stronger encryption, there are much fewer capabilities that are possible.

However, these technologies can be used together, for example, in conjunction with a jammer. Imagine jamming the 3G and 4G signal spectrum, which causes a phone to downgrade to 2G, and then is vulnerable to the widest range of potential attacks. So these downgrade attacks undermine the improved security features that we see in the newer cellular standards.

So with respect to closing the gap, 2G, in my opinion, represents one of the weakest links. The weak encryption and authentication is a major security challenge with modern cell phones. And interestingly, carriers have already decommissioned much of the 2G infrastructure here in the United States. So if carriers were able to push policies to phones that would prevent phones from connecting to vulnerable 2G networks, this would go a long way into addressing this issue. Currently iPhones lack the ability to do this, and with android phones, you have to know a secret number to type in that results in a secret diagnostic menu that allows you to change this setting. Not exactly user-friendly, and I think with improved user interfaces and making this the default, we would make users much more secure.

As we think about downgrade—sort of the decommissioning of 2G, we have to be careful though. Many rural networks still rely on 2G, and there are many devices from vehicle telematics to home alarm systems that rely on 2G networks to provide connectivity.

Lastly would be is if we do want to try and identify the tech and track rogue base stations, it's important to understand the motivation for doing so. There certainly are telltale signs that a base station is a rogue base station, and phones are able to differentiate that with a variety of hardware and software modifications. Also there are standards within the cell phone networks that would allow cell phone carriers to be able to track rogue base station activity. In fact, the new 5G security standards makes a specific recommendation about how this data can be used.

However, when we consider this, we must consider to what end we seek to track down these base stations, to notify the user, to notify the carrier, and if so, how that data should be used.

So looking forward, I recommend the Subcommittee consider the following: first, as 2G network infrastructure is decommissioned, phones should not prefer 2G in any circumstances; next, individuals who are likely targets of foreign intelligence should use phones that meet the needed security countermeasures; and finally, if you do seek to track down IMSI catchers, first address to what end and how that data will be used.

Thank you for the opportunity to address the Subcommittee today, and I look forward to your questions.

[The prepared statement of Dr. Clancy follows:]

**Testimony of Dr. Charles Clancy**

**Professor of Electrical and Computer Engineering, Virginia Tech**

**before the House Committee on Science, Space, and Technology, Subcommittee on Oversight, Hearing on "Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats"**

*June 27, 2018*

Chairman Abraham, Ranking Member Beyer, and Subcommittee Members:

My name is Charles Clancy and I am a professor of electrical and computer engineering at Virginia Tech, where I direct the Hume Center for National Security and Technology. In these roles, I lead major university programs in security, resilience, and autonomy. I am an internationally-recognized expert in wireless security and have held leadership roles within international standards and technology organizations including the Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE). My current research sits at the intersection of 5G wireless, the Internet of Things, cybersecurity, and artificial intelligence.

I am co-author to over 200 peer-reviewed academic publications, to include five books on digital communications; am co-inventor to over 20 patents; and am co-founder of four venture-back startup companies all focused in the wireless and security sectors.

Prior to joining Virginia Tech in 2010, I led a portfolio of wireless research and development programs at the National Security Agency.

It is my distinct pleasure to address this committee on topics of critical national importance.

***Background***

Wireless technologies are an intrinsic component of society. Today's social-mobile Internet provides ubiquitous connectivity and access to information. As the social-mobile Internet evolves into the Internet of Things over the next decade, wireless technologies will become even further ingrained into everything we do.

Security of wireless infrastructure is critical. This includes devices, wireless base stations and access points, and core network infrastructure. Historically cellular infrastructure equipment has been expensive, making it cost prohibitive for most hackers to tinker with wireless systems. As a result sophisticated attacks against wireless networks were the domain of nation-state actors. However

technologies like smallcells and software-defined radio have lowered the price point considerably and led to a significant expansion of public research into cellular network hacking.

While each generation of cellular technology improves security and privacy, the backward-compatibility challenge means that even if we deploy highly-secure 5G networks, most phones can still connect to insecure 2G networks even though many of the national carriers in the US have already decommissioned their 2G infrastructure. This mixture of old and new technologies in devices and carrier networks means that insecurity will always be part of the cellular ecosystem. Combating threats to wireless infrastructure requires a risk management approach that constantly evaluates potential vulnerabilities, observed threats, engineers countermeasures, and communicates best practices.

***IMSI Catcher Technologies***

The terms *IMSI Catcher* and *Stingray* have come to symbolize a range of cellular surveillance technologies and differentiating them is important.

**Rogue base stations**, also known as *cell site simulators*, are devices that act like cell towers from a particular carrier network, but are not part of that network. 2G technology is particularly susceptible to this threat because the authentication in 2G is weak – the network verifies the identity of the phone, but not vice versa – and all the standard encryption modes have been cracked. A 2G rogue base station is able to lure a phone into connecting; elicit its identity, known as its IMSI; prevent it from disconnecting; query the phone's precise GPS location; and intercept voice, data, and SMS content. 3G and 4G rogue base stations are less capable because the underlying standards employ stronger encryption and authentication. A 3G/4G rogue base station is able to elicit a phone's identity, but little else. Earlier this year, 5G adopted a proposal known as "IMSI encryption" that prevents a 5G rogue base station from successfully eliciting a phone's identity. While security has been improving within the standards, backward compatibility in phones means that 2G rogue base stations are still quite effective.

Rogue base stations can be used for a variety of applications, but are most commonly associated with "IMSI catching". They interact with phones for a few milliseconds to learn the phone's identity, and then pass the phone back to the real network. Law enforcement can use the technology to track down criminals. Intelligence and counter-intelligence services can gather data to track the movements of targets. While criminal organizations could theoretically take advantage of the technology as well, to date they have focused primarily on using jammers to disrupt GPS and cell phone networks[1].

1. Mike Brunker, "GPS Under Attack as Crooks, Rogue Workers Wage Electronic War", *NBC News*, 8 Aug 2016.

Another class of device is **cellular interception systems**. These devices passively scan the airwaves, identify active cell bands, and then decode the signals observed in those bands. Note that these systems are not always good at catching IMSIs because the IMSI is only sent over the air when a phone first connects to a network, so an interception system would have to get lucky in order to see an IMSI. Given the encryption in 2G has been cracked, these systems are able to decode all the voice, SMS, and data traffic between phones and 2G networks. For 3G and 4G, voice, SMS, and data are protected by strong encryption and therefore not readable by interception systems.

These technologies can also be used together, and in conjunction with a jammer. For example, if 3G and 4G bands are intermittently jammed, then a victim phone may attach to a rogue 2G base station which would then capture the phone and prevent it from returning to the 3G/4G network once the jamming is deactivated. These downgrade attacks undermine the improved security features in later cellular standards.

***Closing the 2G Gap***

Given its weak encryption and authentication, 2G represents a major security issue with modern cell phones. Similar to how security around WiFi was improved over the past decade with phones providing warnings before connecting to insecure WiFi networks, steps could be taken to treat 2G networks as less trusted.

Carriers who have already decommissioned their 2G networks could push policies to phones that prevent phones from connecting to 2G unless roaming to other networks. Current iPhones lack the ability for users to do this, and Android users need to type a secret code into the phone to open a hidden diagnostic menu in order to disable 2G. Making this the default and giving users more awareness and control through the user interface would address the majority of the operational security and privacy issues associated with 2G.

An important consideration however is rural areas that only have 2G service and legacy devices such as vehicle telematics and home security systems that only support 2G networks. These users and networks cannot be disenfranchised.

***Catching IMSI Catchers***

There have been several studies on how to detect rogue base stations and the proposed approaches generally fall into two categories: phone-based and carrier-based.

The first approach relies on phones to assess whether a base station looks suspicious[2]. Every cell tower broadcasts information about itself, including power levels needed to connect, types of encryption supported, and the identities of its adjacent towers. A rogue base station is likely to indicate that phones should connect at any power level, no encryption is supported, and there are no other towers in the area. These anomalies can be detected by the phone. There are a number of software apps available that purport to perform this task, but they are limited by the amount of cell network metadata provided by Android and Apple to apps[3]. Any reliable solution would need to be baked into device firmware.

Another approach is to leverage data within the network. Phones constantly track the power level of towers within range to determine if they should initiate a tower handover. Phones periodically send this data to the network in what's known as a *measurement report*. The new 5G security standards recommend that these reports can be used by carriers to identify when an unrecognized base station is visible to a phone[4].

Both of these approaches suffer from the "spy-versus-spy" phenomenon whereby improvements in detection technologies result in improvements in spoofing technologies. Any detection strategy would need to constantly evolve as adversary capabilities improve.

Regardless, when considering options for detecting and reporting rogue base stations, one must consider to what end the detection is being performed. If a phone detects a possible rogue base station, should it notify the user? Should the user then notify someone? If a carrier detects a rogue base station should it report it to the FBI? File an interference complaint with the FCC? Given the presumption is that some of these rogue base stations are being used by foreign intelligence and some by domestic law enforcement, how can you tackle the former without negatively impacting the latter? These issues need to be addressed first before the appropriate technical solution can be formulated.

---

2. A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, E. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers", *ACM Annual Computer Security Applications Conference (APSAC)*, December 2014.

3. R. Borgaonkar, A. Martin, S. Park, A. Shaif, J-P Seifert, "White-Stingray: Evaluating IMSI Catchers Detection Applications", *USENIX Workshop on Offensive Technologies (WOOT)*, August 2017.

4. P-K Nakarmi, K. Norrman, "Detecting false base stations in mobile networks", Ericsson Research Blog, 15 June 2018.

***Recommendations***

Looking forward, I encourage this subcommittee to consider the following.

First, carriers that have decommissioned their 2G infrastructure should update phone policies to only connect to 3G/4G networks when not roaming. This will address the majority of the security concerns around cell phone surveillance.

Next, individuals who are likely targets of foreign intelligence should use phones with the needed countermeasures to protect them from cell phone surveillance technologies, such as those recommended by NIST Special Publication 800-187[5] and DOD's Security Technical Implementation Guides for smartphones[6].

Finally, if tracking down IMSI catchers is a desired objective, first address issues with how this information will be used, by whom, and to what end. If the bulk of the risk can be effectively managed by closing 2G gaps and hardening phones for at-risk individuals then the utility of illegal IMSI catchers may decline sufficiently to avoid the need for more systematic approaches to detecting and reporting their operation.

Thank you for the opportunity to address the subcommittee today and I look forward to questions.

5. J. Cichonski, J. Franklin, M. Bartoch, "Guide to LTE Security", NIST Special Publication 800-187, December 2017.

6. Defense Information Systems Agency, "Mobility – Smartphone/Tablet Security Technical Implementation Guides", https://iase.disa.mil/stigs/mobility/Pages/smartphone.aspx

**BIOGRAPHY**

Dr. Charles Clancy is a professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech, and is Director of the Ted and Karyn Hume Center for National Security and Technology. With over 70 faculty and staff, the Hume Center leverages $10M to $15M in annual grants and contracts to engage 350 students in research and experiental learning focused in national security and technology. Additionally, Dr. Clancy leads efforts in developing and expanding the university's role in cybersecurity research and education. Dr. Clancy is an internationally-recognized expert on the security of wireless and cellular networks, and has testified to Congress on cybersecurity issues.

Prior to joining Virginia Tech in 2010, Dr. Clancy spent seven years working for the US Department of Defense in a variety of research, engineering, and operations roles. The majority of his time was spent as a researcher with the Laboratory for Telecommunications Sciences, a federal research laboratory at the University of Maryland. There he led government research programs in wireless communications, with an emphasis on software-defined and cognitive radio. His research focused on efficient use of commodity processors for software-defined radio, and security implications involved in military use of cognitive radio technologies. During this time, Dr. Clancy was also heavily involved in wireless authentication and authorization protocol standardization, and held leadership positions within the Internet Engineering Task Force.

Dr. Clancy received his BS in Computer Engineering from the Rose-Hulman Institute of Technology in 2001, his MS in Electrical Engineering from the University of Illinois, Urbana-Champaign in 2002, and his PhD in Computer Science from the University of Maryland, College Park, in 2006. His studies focused on information-theoretic foundations of communications and security.

An avid entrepreneur, Dr. Clancy is co-founder of a number of companies, including HawkEye 360, focused on commercial space-based RF sensing; Federated Wireless, focused on next-generation wireless and spectrum sharing; Optio Labs, focused in mobile security; and Stochastic Research, a technical consulting firm. Additionally he serves as a founding advisor to DeepSig, a company focused on the intersection of machine learning and signal processing. These companies have collectively raised over $120M in venture capital.

Dr. Clancy is a Senior Member of the Institute for Electronics and Electrical Engineers (IEEE) and holds leadership positions within IEEE's Communications and Signal Processing Societies. He has previously served as an editor for *IEEE Transactions on Cognitive Communications and Networking* and *IEEE Transactions on Information Forensics and Security*. In 2015, Dr. Clancy was elected to be a member of the prestigious AFCEA Intelligence Committee.

Dr. Clancy is co-author to over 200 peer-reviewed technical publications in academic conferences and journals and over 20 patents. His books include *MIMO Radar Waveform Design for Spectrum Sharing with Cellular Systems* (Springer 2016), *Cellular Communications Systems in Congested Environments* (Springer 2017), *Spectrum Sharing between Radars and Communication Systems* (Springer 2017), and *Resource Allocation with Carrier Aggregation in Cellular Networks* (Springer 2018).

Chairman ABRAHAM. Thank you, Dr. Clancy.
Dr. Mayer, five minutes.

**TESTIMONY OF DR. JONATHAN MAYER, ASSISTANT PROFESSOR OF COMPUTER SCIENCE AND PUBLIC AFFAIRS, PRINCETON UNIVERSITY**

Dr. MAYER. Chairman Abraham, Ranking Member Beyer, Ranking Member Johnson, and Members of the Subcommittee, thank you for the opportunity to address cell-site simulators and the broader topic of communication security and privacy at today's hearing.

These issues were central to my recent service as chief technologist of the Federal Communications Commission Enforcement Bureau. They have been an essential component of my computer science and legal research.

In last week's groundbreaking Carpenter v. United States decision, the Supreme Court recognized that "Cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying on is indispensable to participation in modern society." The private sector, the public sector, and the American people all depend on our communications infrastructure. The security and privacy safeguards for that infrastructure have not kept pace with its growing importance to the Nation. Our communications 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 brief opening statement, I will focus on security and privacy risks associated with cell-site simulators. My written testimony highlights several other areas of cybersecurity vulnerability, including insecure call and text message routing, delayed mobile device software updates, and unauthenticated caller ID, the last of which is responsible for the nationwide explosion of fraudulent robocalls.

Cell-site simulators, commonly dubbed IMSI catchers, Stingrays, or dirt boxes, are devices that exploit omissions and mistakes in the trust between mobile devices and cellular towers. 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. The most serious cell-site simulator risks are associated with second generation, or 2G, wireless protocols which were initially deployed in the 1990s and remain operational today to support legacy devices and offer service in rural areas. 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 these cell-site simulators can identify and track nearby mobile devices, 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. And while the latest 5G protocols do include

a new protection against cell-site simulators, that protection is only optional and only effective against some of the known attacks against 3G and 4G networks.

The possible criminal uses of cell-site simulators are limited only by our collective imagination. Criminals could capture private financial information, for example, and steal funds. They could collect sensitive medical information and conduct blackmail. Or they could obtain confidential business information for commercial gain.

Cell-site simulators also pose a serious national security threat. The federal government is the Nation's largest consumer of commercial wireless services, and 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 personnel movements.

In responding to the threat of cell-site simulators, as well as the other serious cybersecurity risks associated with insecure call and text message routing, delayed mobile device software updates, and unauthenticated caller ID, I encourage the members of this Subcommittee to consider leveraging the federal government's communications acquisitions. According to OMB, the United States Government spends about $1 billion every year on wireless service and mobile devices, and yet, as DHS acknowledged in a recent report, the federal government has little assurance that it is paying for wireless service and mobile devices that incorporates cybersecurity best practices. Congress should condition its substantial communications outlays on implementation of appropriate cybersecurity safeguards.

Before I close, I would like to briefly address law enforcement use of cell-site simulators. Federal, state, and local law enforcement agencies use cell-site simulators in the course of criminal investigations, either to track the location of a suspect's mobile device, or to identify all the mobile devices nearby. At present, the federal government owns over 400 cell-site simulators and at least 73 State and local law enforcement agencies also own cell-site simulators. Under current law is a violation of Section 301 of the Communications Act for State or local law enforcement agency to operate a cell-site simulator, because they're transmitting unlicensed wireless spectrum without authorization. Police departments may also run afoul of Section 333, which prohibits wireless jamming because law enforcement cell-site simulators could disrupt 911 calls and other wireless connectivity.

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. But until Congress takes action, the Nation's police departments will remain in legal limbo. I encourage the Members of the Subcommittee to consider legislation that both resolves the Communications Act issues with cell-site simulators, and codifies a warrant requirement for cell-site simulator operation.

Thank you again for the opportunity to address communications security and privacy at today's hearing, and I look forward to questions from the Subcommittee.

[The prepared statement of Dr. Mayer follows:]

**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.

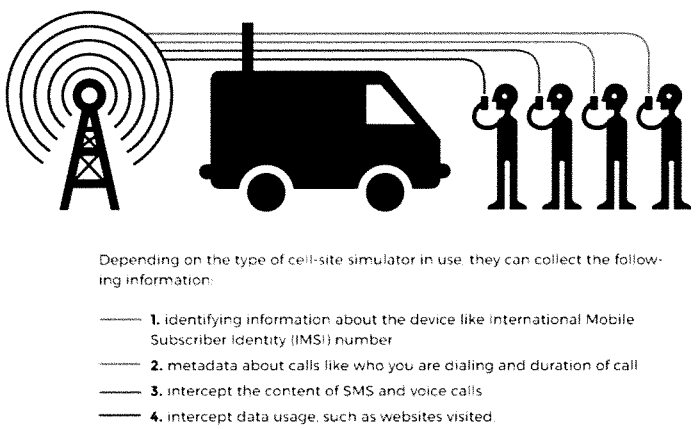
(Intentionally blank.)

[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: When a law enforcement agency operates a cell-site simulator, it conducts a Fourth Amendment search and must presumptively obtain a warrant.[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).

Jonathan Mayer is an Assistant Professor at Princeton University, where he holds appointments in the Department of Computer Science and the Woodrow Wilson School of Public and International Affairs. Before joining the Princeton faculty, he served as the technology law and policy advisor to United States Senator Kamala Harris and as the Chief Technologist of the Federal Communications Commission Enforcement Bureau. Professor Mayer's research centers on the intersection of technology and law, with emphasis on national security, criminal procedure, and consumer privacy. He is both a computer scientist and a lawyer, and he holds a Ph.D. in computer science from Stanford University and a J.D. from Stanford Law School.

Chairman ABRAHAM. Thank you, Dr. Mayer. I thank all the witnesses for that very compelling testimony.

I'm going to recognize myself for five minutes for the opening round of questions. Dr. Clancy, I'll direct my first one to you.

You previously detailed that you see two possible scenarios moving forward with this overall issue. One is a status quo with the possibility of increased training and acknowledgment of these targeted attacks. The second is a substantive dive and to address the issue, which includes a comprehensive assessment of how we treat cell phone towers, permissioned access, and policy changes through updates to phones. Can you provide a little more detail about the difference in the two options, and which would you prefer?

Dr. CLANCY. So I think there are a number of solutions that are possible within this space. There are technical solutions, there are policy solutions, there are legal solutions. I think that there are—the key thing, though, is to ensure that any action that's taken to, I guess, close the gaps that IMSI catchers leverage takes into consideration a path forward for law enforcement around being able to conduct their operations.

So I could imagine scenarios where we essentially look to prevent phones from connecting to IMSI catchers, scenarios where we shut down 2G preference for phones in order to prevent them from being as susceptible to IMSI catchers. But I think any action that we take should be complemented with efforts to ensure that law enforcement still are able to get timely access to location information in order to support their investigations.

Chairman ABRAHAM. Who should lead the effort to have a comprehensive solution to these issues? What set of agencies or people?

Dr. CLANCY. Indeed. So certainly any time we talk about telecommunications and cellular it's tricky because there are so many stakeholders. DHS is the sector-specific agency associated with telecommunications, so they would seem like a logical choice to take the lead. But certainly the FBI, the FCC, and others are key stakeholders in this process.

Chairman ABRAHAM. Okay, thank you.

Dr. Mayer, how does the recent Supreme Court decision on Carpenter v. United States addressing citizens' Fourth Amendment rights change the acceptable use of this technology?

Dr. MAYER. Thank you for the question. Carpenter, by its own terms, does not regulate real time location tracking by law enforcement. The majority was clear on that point. It does, however, express a growing concern by the Supreme Court with the scope of law enforcement capability using modern technology, and to the extent it affects court's views on cell-site simulators, it will only serve to heighten the level of protection.

That said, I want to be very clear to note that to my knowledge, every recent court decision has addressed the question of whether cell-site simulators are regulated by the Fourth Amendment has concluded they are regulated by the Fourth Amendment and a warrant is required for their operation.

Chairman ABRAHAM. Do you think it will have an impact on this—from this Carpenter decision on lawful and legitimate use of the rogue base stations or the IMSI catchers to thwart criminal activity?

Dr. MAYER. So at the federal level I don't believe there will be an effect because by policy, the Department of Justice and the Department of Homeland Security already obtain warrants to operate these devices. At the State and local level, my understanding is that some police departments do currently operate these devices without obtaining a search warrant, and they may continue to do those things notwithstanding the Carpenter decision. This issue has not been fully litigated in every jurisdiction.

Chairman ABRAHAM. Dr. Romine, NIST has published the Mobile Threat Catalog which provides incredible useful information about the overall issue of mobile device security. How is NIST getting this information out and in front of vendors and people that need to see it?

Dr. ROMINE. Thank you, Mr. Chairman.

We have a collection of stakeholders that are in contact with us on a regular basis. We have thousands of people who subscribe to our newsletters. In general, those are stakeholders that are monitoring the work that we do. We are working through the Standards Development Organizations, the 3GPP, for example, which has a lot of the work that we're doing and involves trying to help improve the security of telecommunications activities and their channels associated with getting the information out through those mechanisms as well. We also manage an active website with many, many—tens of thousands of hits on a regular basis for people who are looking at what we're doing in cybersecurity broadly and for specific topic areas as well.

Chairman ABRAHAM. Is NIST working with other government agencies to promote this, such as a cybersecurity framework?

Dr. ROMINE. Well, it is not directly related to the cybersecurity framework, but we are working with other federal agencies. We encourage a large number of agencies to work, for example, in the standards development bodies so that all of the requirements and associated concerns can be expressed in those bodies.

Chairman ABRAHAM. Okay, thank you.

Mr. Beyer.

Mr. BEYER. Thank you, Mr. Chairman, and it's nice to have a Chairman from Texas that loads the panel up with Virginians.

So Dr. Romine, your PAC from UVA is very much appreciated. Dr. Clancy teaching with the Hokies at Virginia Tech. Dr. Mayer, I'm sorry about the Stanford Princeton background, you know, but you can—they can slum it today.

Dr. MAYER. I enjoy visiting the state.

Mr. BEYER. That's good. Dr. Mayer, you know, according to press reports the President frequently uses his unsecured cell phone and routinely refuses to change that to an official secured phone. That was one of the recommendations that people in very sensitive roles have these highly secure phones. We talked about the cell phone number to Kim Jong-un.

Can you describe why these practices may put the President's phone at risk from being hacked or penetrated by foreign intelligence agencies?

Dr. MAYER. Any senior official in any of the branches of government—and for that matter, any senior executive in the private sector—should take heightened precautions with respect to their tele-

communications equipment. There are possible attacks involving interception of voice and text messages. In my written testimony, I describe how those might proceed. There are also the cell-site simulator risks that we've discussed. And in addition, there's an issue of security updates not necessarily getting delivered in a timely fashion to consumer devices, such that they could be remotely compromised.

So there are a number of cybersecurity risks that are very significant in this ecosystem that could result in essentially total compromise of communications, and again, anyone in a sensitive position should take heightened precautions.

Mr. BEYER. Great, thank you very much.

Dr. Romine, in Dr. Mayer's presentation he talks about femtocells, consumer hardware sold by wireless providers that extend coverage indoors and into rural areas. Are these the things I bought from Google that allow my wife to use her wireless thing upstairs?

Dr. ROMINE. I think that's probably a good example of exactly what was described.

Mr. BEYER. So one of the things that we consumers may have been totally unaware of is by buying essentially the wireless extenders within our home, that we have set up these rogue IMSI devices?

Dr. ROMINE. I'd have to double check the particulars, but I don't think that's quite the same kind of thing that we're talking about. In the case of these devices, these are lawfully provisioned to provide extended coverage and are not considered camping illegally on spectrum that hasn't been authorized.

Mr. BEYER. I wasn't so worried about us breaking the law as we were setting up bad guys to get our——

Dr. ROMINE. Oh, I see what you're saying. I don't know the particulars of the femtocells and whether they have similar kinds of cybersecurity built into them. I think it would depend on the manufacturer and on the way that they're provisioned. I'll have to get back to you on whether I think there's additional vulnerability associated with having femtocells in your home.

Mr. BEYER. Great. Dr. Clancy, I loved your recommendations at the end. You talked about the default setting that the major phone carriers need to set default stuff within the androids and the iPhones that would basically disable the 2G thing unless they're specifically roaming. How do we make that happen? Is there a role for Congress there?

Dr. CLANCY. That's a good question. It's a fairly simple change to the software of the devices. It could even be done as a policy push from the carrier networks.

Right now, users have the ability to shut off 3G and 4G particularly on iPhones, but they do not have the ability to shut off 2G, which is sort of backwards in my opinion. So with some minor policy shift pushes from the carriers that have already decommissioned 2G, these devices would default to only using 3G and 4G.

Mr. BEYER. Is this something that they could tell all of us with our iPhones and androids to do, or do you have to do that in the units they sell going forward?

Dr. CLANCY. Well it would need to be an update that they push from the networks to the phones. It wouldn't necessarily just be new devices. There is not a way for a user to do it by themselves within the current infrastructure. Even the secret code I talked about that brings up the diagnostic menu where you can change it yourself, it doesn't—once you reboot your phone, the setting goes away so you have to sort of constantly go in and make sure that 2G is disabled.

So there are some very simple things that could be done with the user interface through software updates that would cause phones to not connect to 2G unless roaming.

Mr. BEYER. Okay, great. Mr. Chairman, I yield back.

Chairman ABRAHAM. Thank you.

Mr. McNerney?

Mr. MCNERNEY. Well I thank the Chair and I thank the witnesses. I apologize for leaving during your testimony, but you did have written testimony that we reviewed beforehand.

My question is similar to Mr. Beyer's question, the Ranking Member's question. Dr. Mayer, in your testimony you state that the most serious cell-site simulator risks are associated with 2G wireless protocols, which were deployed in the 1990s and remain operational today to support the legacy devices that are out there. Who are the consumers that are most likely to possess these legacy devices?

Dr. MAYER. Well as Dr. Clancy testified, there are a number of devices like home alarm systems, connected devices that were deployed in the 1990s or early 2000s that just don't have newer cellular technology built into them. Nowadays we call these things the internet of things, but back then it was just your alarm system.

So those are the types of devices that might be affected, and it's also important to note that rural connectivity is sometimes provided by 2G, because those networks were built out and have not been updated since.

That said, I think providing the security protection associated with disabling 2G need not come at the expense of disabling those legacy devices or rural connectivity. You know, for folks who live in an area that doesn't have 2G—or that has 3G, 4G, or now 5G coverage, disabling 2G wouldn't be a problem.

Mr. MCNERNEY. But there are a lot of legacy devices out there that they are going to continue to require 2G protocols, right?

Dr. MAYER. I'm afraid I don't have a handle on the scale of the use of 2G networks at this point, but it is not an area where we have to make a tradeoff between supporting those devices and securing the latest devices. We can do both.

Mr. MCNERNEY. Well you note that while most 3G and 4G protocols include authentication for cell towers, they still have significant site cell tower vulnerabilities. Could you expand on that a little bit?

Dr. MAYER. Sure. In my written testimony, I describe three classes of vulnerability in addition to taking advantage of 2G networks. One class of vulnerability is location tracking. There are certain components of the 3G and 4G cellular protocols that enable location tracking, even though the base station isn't properly authenticated. So that's one class of attack.

Another class of attack is taking advantage of femtocells, as Ranking Member Beyer noted. These are home devices that serve as range extenders. Criminals could compromise these devices and convert them into their own cell-site simulators, and in fact, researchers have demonstrated that this can actually be a pretty easy thing to do.

The third class of attack I describe takes advantage of either collaborating with or compromising a foreign cellular network, and then effectively tricking devices within the United States into roaming on that foreign network.

So there are multiple other categories of attack in addition to the 2G issue.

Mr. MCNERNEY. So these range extenders, when they're attacked, does that give the attacker just access to the person that has the range extender or does it go beyond that?

Dr. MAYER. Those devices could give access to any person targeted by whoever's operating the range extender that's been compromised, and that could allow intercepting voice, intercepting text messages, and intercepting data.

Mr. MCNERNEY. Thank you.

Dr. Clancy, when a carrier detects the rogue base station is in operation, is it currently required to report that to an agency like the FBI?

Dr. CLANCY. Currently the carriers perhaps are collecting enough data to make that determination, but they are not archiving it in a way that it can be analyzed to produce that conclusion. So there is sort of data that exists ephemerally within the carrier networks that could be a telltale sign that an IMSI catcher is operating in their geographic footprint. Right now that data is not being stored. It is not being analyzed, and it is only now in the 5G standards that it is even proposed that that is a thing that should be done. So I think that is sort of unexplored at this moment in terms of what should be done with that data.

Mr. MCNERNEY. Is that a business opportunity or a regulatory opportunity to control that?

Dr. CLANCY. So there are other countries where that data is handed over to third parties and use for all manners of analytics. I think those countries have substantially different privacy laws than we do here in the United States, so I think it is data, certainly given all the focus on cellular privacy we have seen over the last few weeks, that I wouldn't necessarily consider a business opportunity. It would need to be treated carefully.

In terms of regulatory, yeah, I mean, I assume you could regulate that data needed to be analyzed, and if detection was—if you discovered a rogue base station then you should tell someone. I guess the question is who? Do you file an interference complaint with the FCC? Do you file something with the FBI saying that you've detected an IMSI catcher? These things, of course, could be being used by—lawfully by federal law enforcement, or they could be being used unlawfully. And the carrier wouldn't know which it was.

Mr. MCNERNEY. Mr. Chairman, I'll yield back.

Chairman ABRAHAM. All right. Well so I'm thinking of ditching my cell phone and going to get two cans and a string to—you have some questions, Mr.——

Mr. BEYER. Well I was going to yield to either of you guys.

Chairman ABRAHAM. I'm going—we're going to have a second round of questions now, so we're good. Okay. Yeah, we're—this is such an interesting topic, we're going to continue here for at least another round.

Dr. Mayer, is it possible to attribute any legal cell-site simulator to a particular actor, specifically particular cell-site simulators, do they have characteristics associated with where they were made or the entity using them? For example, if the device was made in China or in Russia, would it have any specific identifiers?

Dr. MAYER. That's a great question, Chairman Abraham. I'm not aware of any instance in which a law enforcement or regulatory agency has successfully tracked down one of these devices, and so I'm not aware of anyone who's tried to attribute one of these devices once they get their hands on it or having studied the signals emanating from it and concluding that it was definitively a cell-site simulator.

And so I think in principle it could be possible to attribute one of these devices. Again, I'm not aware of an instance in which folks have gotten close enough to do that.

Chairman ABRAHAM. Dr. Clancy, do you have anything to add to that?

Dr. CLANCY. So in my experience, there's broadly two classes of these devices. There are the expensive ones that are manufactured principally for military and law enforcement use, and their signaling parameters would likely have one set of characteristics associated with it. There's another that's based on inexpensive open source hardware and software that you would likely find being used potentially by foreign intelligence. It depends on the sophistication level of the adversary.

I would imagine that you could, with relative simplicity, tell the difference between an open source—one that was built on open source software versus one that was built for higher end military and law enforcement use, and I would imagine that that would also then be differentiable from the legitimate cell tower networks.

Chairman ABRAHAM. Okay, Dr. Mayer, back to you. In your testimony, you state that to your knowledge, other than the recent DHS pilot project, no component of the U.S. Government has acknowledged a capability to detect cell-site simulators in the field, including wireless carriers.

Additionally in a response to Senator Wyden, DHS specifically claimed it did not currently possess the technical capability to detect cell-site simulators. Should DHS have this capability, and if so, how difficult would it be for them to actually have it?

Dr. MAYER. So there are commercial tools available for law enforcement and regulatory agencies to attempt to detect these devices. The inherent challenge with detecting these devices is that there is no definitive telltale sign of a cell-site simulator. There are only indicia that give rise to suspicion, that the tower appears to be configured in an unusual way, and it appears to be broadcasting on unusual spectrum or unusual power level. But there are many

reasons why legitimate cell towers are configured in unusual ways, either intentionally or unintentionally. They may appear and disappear, such as getting set up for a special event, and so again, while there are commercial tools available, I'm not aware of anyone who's used any of these tools to definitively identify one of these devices, and that's why my recommendation is focusing on defense rather than whack-a-mole with the folks setting these things up.

Chairman ABRAHAM. Dr. Clancy, in its mobile device security study, DHS concluded that it "believes"—and I will put that in quotes—"that all U.S. carriers are vulnerable" to the SS7 and the Diameter attacks, in addition to the federal government having little assurance that it's paying for cellular service and mobile devices that incorporate cybersecurity best practices. Since DHS has responsibility for the protection of critical infrastructure of the government, in your opinion, should DHS continue researching the risks through pilot programs and studies like the 2017 pilot? What DHS S and T be—would be the appropriate division to continue this research?

Dr. CLANCY. So within DHS SNT, there would be two logical groups. There's a public safety group and there's a cybersecurity group. Perhaps it would be an interesting collaboration between the two that could focus on these topics.

I do think that there's room for continued research on developing and maturing these tools. I do also agree that the sort of whack-a-mole approach is—would be challenging. Anytime you identify what you think is a unique signature for one of these devices, a sophisticated adversary could change that signature in order to avoid detection.

So I'll also note that there are apps that are available that purport to identify a rogue base station, and there was a systematic study done last August—it was published last August which showed that they were able to fool all of those apps into thinking that their rogue base station was indeed a legitimate one. So again, supporting this notion that whack-a-mole would be challenging against a sophisticated adversary.

Chairman ABRAHAM. Mr. Beyer.

Mr. BEYER. Thank you, Mr. Chairman.

Dr. Mayer, you wrote that in 2016 the major wireless carriers committed to targeting a rollout for caller ID authentication in the first quarter of 2018, and as of today, not a single major wireless carrier has adopted rigorous caller ID authentication. Can you tell us why? Is it ridiculously expensive? Have they been otherwise distracted? AT&T, for example.

Dr. MAYER. Ranking Member Beyer, before answering that in just a moment, if I might add to Dr. Clancy's response on the last question that our allies across the pond in the United Kingdom actually have their government audit communications carriers to make sure that these SS7 and Diameter vulnerabilities have been addressed. The notion of DHS jumping into the carriers maybe is not—may be worth further discussion, but at any rate, our allies have a different approach to this than we do.

With respect to the robocall issue and call authentication, my understanding is that the carriers are not eager to make new investments in what they view as a declining area of their business. The

growth in cellular communications has been in data and not in voice, and so investing new money in voice security is a bit of a tough proposition when these are systems that are just not going to be revenue generators in the future.

Mr. BEYER. Despite the fact that there are billions of robocalls made that harass Americans every year?

Dr. MAYER. That's right, and I think an extra dimension of this that I will certainly I find personally frustrating is the major wireless carriers not only have not taken steps to address the issue, but in fact, charge a monthly fee if you would like to use their services to address robocalls.

Mr. BEYER. Wow. Thank you very much.

Dr. Clancy, you write that criminal organizations could theoretically take advantage of the technology, but they haven't. Why not?

Dr. CLANCY. Well it depends on—in order to take advantage of the technology, you need a fairly sophisticated sort of intelligence analysis function. If you're simply catching IMSIs, you have to know to whom those IMSIs belong, and that isn't readily available if you're just doing this opportunistically.

So law enforcement and foreign intelligence are spending a lot more time on the analytic component in order to develop those relationships and know what IMSI they're looking for, whereas criminal organizations don't often have the analytic capacity to accomplish that, so they've been focused on more brute force technologies like just jamming the cellular signals in order to accomplish their acts.

Mr. BEYER. Okay.

Dr. CLANCY. At least that's been my observation.

Mr. BEYER. Thank you.

Dr. Romine, I think it was Dr. Mayer who wrote that other than the DHS pilot, no component of the United States government has acknowledged the 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. Is this a hole in our federal capabilities, and where does NIST fit into this?

Dr. ROMINE. Thank you for the question. Let me address the second part of that first, which is that NIST's role in this space, is to strengthen the security of telecommunications networks, and we do that principally through our engagement with the standards development process and in the guidelines that we publish, such as the special publication I referenced in my testimony, to try to provide useful input for operators and others who might like to strengthen their telecommunications activities.

The question of the gap, or if there is a gap in this, is probably a little above my pay grade. I don't know what the right answer to that is. I would say that certainly the Department of Homeland Security has a role to play as the sector-specific agency for the telecommunications sector. Beyond that, it's not clear to me.

Mr. BEYER. Thank you. Dr. Mayer, you wrote that paragraph. What was your intent in talking about this gap?

Dr. MAYER. My view is that while it is worth spending time on attempting to improve detection of these devices, the far better or far more effective focus for federal policy would be on defense. We

know how to defend against the worst of these attacks, and I think it is a—it would be a very reasonable thing for Congress to say when we're spending all this taxpayer money on wireless services and devices, we expect at minimum defenses against the worst of the worst.

Mr. BEYER. I agree. Thank you very much.

Mr. Chairman, I yield back.

Chairman ABRAHAM. Thank you, Mr. Beyer.

Mr. McNerney?

Mr. MCNERNEY. Again, I thank the Chair for another round of questions.

Dr. Romine, in your testimony you noted that 4G systems have a number of operational capabilities that mobile network operators may choose to implement, and that's presumably to secure cell phone communications. Has NIST conducted an analysis to determine what has been implemented to date, how widespread that implementation is, and what's still needed?

Dr. ROMINE. Thank you, sir. We have not done that analysis. We don't do operational activities. We're not a provider of these services and we don't have any insight into way the operators are currently using these, and whether the optional security features or privacy features are being turned on or not.

From our perspective, I agree with the other two witnesses here that there's some low-hanging fruit here. The easiest part of this, or the most important, would perhaps be addressing this idea of dropping back to 2G communications—and I want to be clear here. The vendors or the mobile operators are not doing this because of any lack of understanding of the concern of security. They are doing it to provide the best user experience, right? So the vulnerability exists because the telecommunications providers are trying to ensure a seamless communication.

That said, I think it's going to take a collaboration among users, vendors, and the industry to ultimately complete the phaseout of 2G communications.

Mr. MCNERNEY. That's what it's going to take, phasing out the 2G communications?

Dr. ROMINE. That's certainly one major focus that I think would make a difference.

Mr. MCNERNEY. Thank you. Dr. Clancy, you said that in the past, both industry and the federal government need to significantly increase cybersecurity funding research. You said that the Government often approaches cybersecurity with an "after the fact solutions applied with duct tape and bubble gum." You also said that cybersecurity investments by both the federal government and industry are drastically underfunded. Do you have any specific recommendations on funding levels or investments in federal cybersecurity R&D, or comments on what the federal government can do better to address our cybersecurity research efforts?

Dr. CLANCY. So as an academic, it's always—I think I'm congressionally required to lobby for more university research funding.

Mr. MCNERNEY. Yeah.

Dr. CLANCY. But no, seriously, I think that there is a critical need for continued investment in cybersecurity. The World Economic Forum states that cyber risk is the number one risk to inter-

national organizations doing business in the United States. This is the challenge of our time and needs to be the focus of significant R&D investment, particularly in the cellular spaces where the majority of the R&D investment is happening in the EU. The Horizon 20/20 program out of the EU is funding almost all of the 5G security research right now, and we have very little being funded here in the United States, either through the National Science Foundation or DHS. And that seems like a key opportunity for the U.S. to take a leadership role in an area as important as this.

Mr. MCNERNEY. Well it's our responsibility to decide how much money to spend on these things, and we need guidance. So if there's a place we can go to find that kind of guidance, I think it would be very useful.

Dr. Clancy, you have said the United States needs for one million cybersecurity-related jobs, that an estimated 31 percent of those jobs are vacant now. You also pointed out the fact that American universities are not offering the right kind of courses to train people in cybersecurity. Do you have any recommendations for Congress to try and help energize efforts for the right source of—sorts of computer security expertise that our nation needs?

Dr. CLANCY. So yes, there are——

Mr. MCNERNEY. Similar question.

Dr. CLANCY. There are currently, what, 300,000 empty cyber jobs across the country. Here in the DC. region, we have 42,000 unfilled cyber jobs. We have the densest cyber workforce in the world here in the DC. region, and among the highest vacancy rate because the talent is so sought after.

So there's a range of different activities that are needed to invest in workforce development programs. The number of new cyber jobs that are needed each year exceeds the number of students graduating with a degree in computer science each year, so this needs to be not just viewed as a computer science domain, this is a domain for business and policy. A wide range of skills are needed in order to effectively combat this challenge.

So for example, there are federal programs such as the Cyber Course Scholarship for Service Program that is administered by OPM and the National Science Foundation. I think opportunities to expand that program to focus beyond the pure technical skills of computer science would be an opportunity to densify the workforce pipeline.

Mr. MCNERNEY. And you—would you think that there's a significant opportunity for women and underserved minorities to—in this field?

Dr. CLANCY. Certainly. So cybersecurity is notorious for its poor performance in diversity, both in terms of gender and racial background. So I think programs specifically targeting women and underrepresented minorities in order to increase awareness are critical, and most studies have found that this isn't something you can't start at college. This has to go all the way back to third and fourth grade where people are sort of beginning to decide whether or not a STEM career is what they want to pursue or not.

Mr. MCNERNEY. Thank you, Mr. Chairman.

Chairman ABRAHAM. All right, good stuff.

I thank the witnesses for their testimony, very valuable, and Members for their great questions. The record will remain open for two weeks for additional comments and written questions from members.

This hearing is adjourned.

[Whereupon, at 3:24 p.m., the Subcommittee was adjourned.]

# Appendix II

## Additional Material for the Record

LETTER SUBMITTED BY REPRESENTATIVE RALPH LEE ABRAHAM

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

June 27, 2018

The Honorable Ralph Abraham, Chairman
The Honorable Don Beyer, Ranking Member
House Committee on Science, Space, and Technology
Subcommittee on Oversight
2321 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Abraham and Ranking Member Beyer:

We write to you before the hearing "Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats."[1] In a landmark ruling last week, the U.S. Supreme Court held that the Fourth Amendment protects location records generated by mobile phones.[2] As a consequence, Congress should update privacy law to address the challenges of devices such as Stingrays. StingRays, with their ability to discretely collect vast troves of non-target, non-pertinent data should clearly be subject to the heightened Title III warrant requirement for communications interception.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC has a particular interest in the impact of new surveillance technologies with the capacity to enable warrantless, pervasive mass surveillance of the public by law enforcement agents. EPIC has long promoted oversight of IMSI Catchers, or "StingRays," by law enforcement agencies. An EPIC FOIA lawsuit in 2012 revealed that the FBI was using StingRays without a warrant, and that the FBI provided StingRays to other law enforcement agencies.[4] EPIC has also filed amicus briefs in federal and states courts arguing that cell phone location data is protected by the Fourth Amendment.[5]

A StingRay is a device that can triangulate the source of a cellular signal by acting "like a fake cell phone tower" and measuring the signal strength of an identified device from several locations. With StingRays and other similar "cell site simulator" technologies, Government

---

[1] *Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats*, 115th Cong. (2018), H. Comm. on Science, Space, & Technology, Subcomm. on Oversight (June 27, 2018), https://science.house.gov/legislation/hearings/subcommittee-oversight-hearing-bolstering-data-privacy-and-mobile-security.
[2] *Carpenter v. United States*, 585 US _ (2018).
[3] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] *EPIC v. FBI*, No. 12-667 (D.D.C. Mar. 28, 2013); *See generally* https://epic.org/foia/fbi/stingray/.
[5] *See e.g.* Brief of Amici Curiae EPIC et. al,, *Carpenter v. United States*, 585 US _ (2018) (arguing that the Fourth Amendment protects the right against warrantless seizure and search of location data), *available at* https://epic.org/amicus/location/carpenter/Carpenter-v-US-amicus-EPIC.pdf.

investigators and private individuals can locate, interfere with, and even intercept communications from cell phones and other wireless devices. the use of cell site simulator technology implicates not only the privacy of the targets of investigation, it also affects other innocent users near the technology. And their abilities go far beyond location tracking, including the ability to intercept, redirect, spoof, otherwise modify the content of calls.

After EPIC's 2012 FOIA lawsuit, the Justice Department released new guidelines that require the Department's law enforcement components to obtain a warrant before using Stingrays.[7] The policy prohibits officers from using Stingrays to intercept communications, and requires that all non-target data be deleted after use. And last year, a federal court ruled that warrantless use of a stingray violates the Fourth Amendment.[8]

Because StingRays can (1) collect data about all devices in an area, (2) enable ongoing monitoring and massive data collection absent clear limits, and (3) potentially interfere with legitimate signals, including emergency calls, the use of these devices by law enforcement should be subject to the same heightened "super warrant" requirement placed on Wiretap Orders since Congress passed Title III in 1968.

We ask that this Statement from EPIC be entered in the hearing record. We look forward to working with you on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Alan Butler*
Alan Butler
EPIC Senior Counsel

/s/ *Christine Bannan*
Christine Bannan
EPIC Policy Fellow

[7] *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, Dept. of Justice (2015), *available at* https://www.justice.gov/opa/file/767321/download.
[8] *Jones v. U.S.*, 168 A.3d 703 (D.C. App. 2017).

ARTICLES SUBMITTED BY REPRESENTATIVE
DONALD S. BEYER, JR.



# Trump ramps up personal cell phone use

By Pamela Brown and Sarah Westwood, CNN

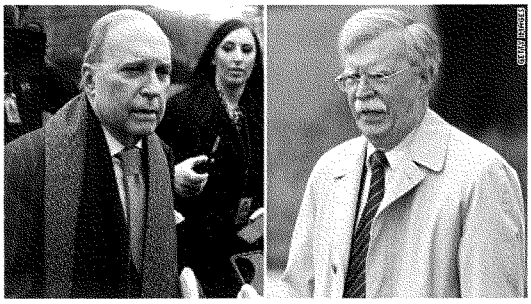
Updated 12:00 PM ET, Tue April 24, 2018

Sources: Trump increasingly uses personal cell 01:33

**(CNN)** — President Donald Trump is increasingly relying on his personal cell phone to contact outside advisers, multiple sources inside and outside the White House told CNN, as Trump returns to the free-wheeling mode of operation that characterized the earliest days of his administration.

"He uses it a lot more often more recently," a senior White House official said of the President's cell phone.

Sources cited Trump's stepped-up cell phone use as an example of chief of staff John Kelly's waning influence over who gets access to the President. During the early days of Kelly's tenure, multiple sources said, Trump made many of his calls from the White House switchboard -- a tactic that allowed the chief of staff to receive a printed list



**Related Article:** Bolton, Kudlow on the rise, but risks abound

Three sources familiar with the situation said Trump has also increased his direct outreach to GOP lawmakers over the past several weeks, sometimes employing his cell phone.

"Basically, at this point, he's just sort of engaging on his own," observed a source familiar with Trump's calls to congressional allies.

"Kelly used to be more clearly the gatekeeper than he is now from a Hill standpoint," that source added, noting members would typically call Kelly's office if they wanted to set up a talk with Trump rather than dial the President directly.

"I don't know that he even is running it by the chief of staff anymore," the staff said.

Some White House allies said they see Trump's more frequent solicitation of advice outside the West Wing as a sign that Kelly's status as a gatekeeper for the President has diminished.

"Definitely, the walls are breaking," one source close to the White House said of the procedures Kelly initially established to regulate access to Trump. Another source close to the White House added that "a lot of meetings, a lot of things have happened lately without Kelly being in the room."

Former campaign manager Corey Lewandowski has been one notable beneficiary of Kelly's loosened grip. One source said Lewandowski recently bragged to friends that he now enjoys "unfettered" access to the President -- including a recent dinner in the residence with Trump, according to two sources. Upon his arrival last year, Kelly attempted to limit Lewandowski's access to Trump from the nearly unchecked privileges he enjoyed at the start of the administration, although Kelly's efforts were never entirely successful. Lewandowski did not respond to a request for comment.

Trump has also made clear that Larry Kudlow, his new economic adviser, and John Bolton, his new national security adviser, are "direct reports" to him and not to Kelly, two sources familiar with the matter told CNN. Their predecessors, however, reported directly to the chief of staff or at least looped Kelly in after a meeting with the President -- a potential sign of Trump's shift toward controlling more of what goes on in his own White House.

A senior White House official said Kelly's absence from phone calls and meetings in recent weeks is more a reflection of the balance Trump and his chief of staff have struck since Kelly took the job.

"They've grown into some level of comfort," the official said. "There used to be a level of babysitting, and it wasn't organized." The source added Kelly "spent months" fixing the operational process and noted now, Kelly doesn't need to insert himself into as many issues.

## Security questions

"Because the smartphones of high-level government officials -- including the President -- are obvious targets for foreign intelligence services, the government goes to significant effort to ensure that government-issued smartphones are constantly updated to address security vulnerabilities," she said. "Use of personal smartphones, which may not have all of the security features of government-issued smartphones or be regularly updated to address newly discovered vulnerabilities, present an obvious potential security risk."

Another security expert said the President's increased cell phone use makes his calls more vulnerable to eavesdropping from foreign governments.

"All communications devices of all senior government officials are targeted by foreign governments. This is not new," said Bryan Cunningham, executive director of the Cybersecurity Policy and Research Institute at the University of California-Irvine.

"What is new in the cell phone age is the ease of intercepting them and that at least our last two presidents ... have chafed at not being able to use their personal cell phones," Cunningham added. "Of course, calls are only secure if both parties use a secure device."

Another implication of Trump's private cell phone use, Cunningham noted, is the possibility that Trump's conversations may not be "captured for the purposes of government accountability and history."

POLITICO

POLITICO

WHITE HOUSE

# 'Too inconvenient': Trump goes rogue on phone security

The president has kept features at risk for hacking and resisted efforts by staff to inspect the phones he uses for tweeting.

By ELIANA JOHNSON, EMILY STEPHENSON and DANIEL LIPPMAN | 05/21/2018 07:00 PM EDT

President Donald Trump talks on the phone aboard Air Force One during a flight to Philadelphia on Jan. 26, 2017. | Shealah Craighead/Official White House Photo

President Donald Trump uses a White House cellphone that isn't equipped with sophisticated security features designed to shield his communications, according to two senior administration officials — a departure from the practice of his predecessors that potentially exposes him to hacking or surveillance.

The president, who relies on cellphones to reach f
security around his phone use, according to the a

Listen to Story

The president uses at least two iPhones, according to one of the officials. The phones -- one capable only of making calls, the other equipped only with the Twitter app and preloaded with a handful of news sites — are issued by White House Information Technology and the White House Communications Agency, an office staffed by military personnel that oversees White House telecommunications.

While aides have urged the president to swap out the Twitter phone on a monthly basis, Trump has resisted their entreaties, telling them it was "too inconvenient," the same administration official said.

The president has gone as long as five months without having the phone checked by security experts. It is unclear how often Trump's call-capable phones, which are essentially used as burner phones, are swapped out.

President Barack Obama handed over his White House phones every 30 days to be examined by telecommunications staffers for hacking and other suspicious activity, according to an Obama administration official.

The White House declined to comment for this story, but a senior West Wing official said the call-capable phones "are seamlessly swapped out on a regular basis through routine support operations. Because of the security controls of the Twitter phone and the Twitter account, it does not necessitate regular change-out."

Trump's call-capable cellphone has a camera and microphone, unlike the White House-issued cellphones used by Obama. Keeping those components creates a risk that hackers could use them to access the phone and monitor the president's movements. The GPS location tracker, however — which can be used to track the president's whereabouts — is disabled on Trump's devices.

The West Wing official refuted the idea that the presence of a camera and microphone on the president's phone posed any risk, telling POLITICO, "Due to inherent capabilities and advancement in technologies, these devices are more secure than any Obama-era devices."

Trump's reluctance to submit to White House security protocols that would limit his ability to tweet or contact friends freely is a case of the president's personal peculiarities colliding with the demands of his office — a tension created in part because of society's growing attachment to mobile technology over the past decade.

Obama, who relied on email and text messages, was the first president to speak publicly about his desire to hang on to his cellphone in office and to be photographed repeatedly with it in hand. Trump, who doesn't use email in office, entered the White House eight years later with a long-established Twitter habit and a lifelong attachment of doing business, dealing with the press and gabbing with associates over the phone.

Former national security officials are virtually unanimous in their agreement about the dangers posed by cellphones, which are vulnerable to hacking by domestic and foreign actors who would want to listen in on the president's conversations or monitor his movements.

"Foreign adversaries seeking intelligence about the U.S. are relentless in their pursuit of vulnerabilities in our government's communications networks, and there is no more sought-after intelligence target than the president of the United States," said Nate Jones, former director of counterterrorism on the National Security Council in the Obama administration and the founder of Culper Partners, a consulting firm.

While the president has the authority to override or ignore the advice provided by aides and advisers for reasons of comfort or convenience, Jones said, "doing so could pose significant risks to the country."

Trump campaigned in part on his denunciations of Hillary Clinton's use of a private email server as secretary of state — a system that made classified information vulnerable to hacking by hostile actors.

"Her server was easily hacked by foreign governments, perhaps even by her financial backers in communist China — sure they have it — putting all of America and our citizens in danger, great danger," Trump said in a June 2016 speech in which he called Clinton "the most corrupt person ever to run for president." He repeatedly vowed on the trail to "lock her up."

**White House doubles down on Trump's 'animals' comments**
By MATTHEW NUSSBAUM and CHRISTOPHER CADELAGO

Dozens of Trump's friends and advisers testify to his frequent cellphone use. Florida Rep. Matt Gaetz, a Trump confidant, told POLITICO in April that he hears from the president either late at night or early in the morning, sometimes from a blocked number and sometimes from "a 10-digit number that starts with a 202 area code."

Three White House aides confirmed that Trump's cellphone number changes from time to time. Several aides close to the president also carry secure devices from which he can place calls — a standard practice in any presidential administration.

Trump's chief of staff John Kelly has cracked down on personal cellphone use by White House staff, citing security risks.

Personal cellphones were banned from the West Wing in January in order to "protect White House information technology infrastructure from compromise and sensitive or classified information from unauthorized access or dissemination," according to a memo sent to staff.

The memo was sent after Kelly's own phone was apparently compromised during the Trump transition. At the time, according to a senior administration official, he was told to replace the phone — his own personal device — though he didn't do so until October, after POLITICO reported the potential hacking.

Though it was unclear whether Kelly's phone was compromised by a foreign government, cybersecurity experts pointed to sophisticated adversaries like Russia and China as the biggest threats, and expressed shock over the president's refusal to take measures to protect himself from them, particularly when engaged in delicate negotiations.

"It's baffling that Trump isn't taking baseline cybersecurity measures at a time when he is trying to negotiate his way out of a trade war with China, a country that is known for using cyber tactics to gain the upper hand in business negotiations," said Samm Sacks, a China and technology expert at the Center for Strategic and International Studies.

Former government officials from Republican and Democratic administrations expressed astonishment that any White House would issue the president a cellphone that posed a security threat.

"This would be the case of a president overruling literally the most rudimentary advice given by the communications agencies," said Andrew McLaughlin, who served as deputy chief technology officer under Obama and helped develop the former president's specialized phone.

**Trump victory lap ignores trade time bomb**
By BEN WHITE

Defense Secretary Jim Mattis has warned of the threats posed by unsecured devices and is considering banning personal cellphones as well as exercise trackers from the Pentagon. "It's about electronics, GPS-enabled electronics. You have to also consider the fact that we have been attacked, bases have been attacked. Information is power and our adversaries have used information to plan attacks against us," Mattis spokeswoman Dana White told reporters in early February.

Trump is not the first president to struggle with the relative isolation of the Oval Office and cling to his cellphone as a way to stay connected with friends and family outside of Washington. Three days before his inauguration in 2001, George W. Bush sent a wistful message to friends announcing that he would no longer use email. "Since I do not want my private conversations looked at by those out to embarrass, the only course of action is not to correspond in cyberspace. This saddens me," he wrote them.

Eight years later, Obama begged advisers to find a way for him to keep his beloved BlackBerry after his election and said publicly he used the phone as a way to reach beyond the Washington bubble.

A notorious text and email junkie who was frequently spotted on the campaign trail with headphones plugged in his ears listening to music streaming from his phone, Obama tasked his transition team with developing a phone that complied with the White House's stringent electronic security guidelines. "I'm still clinging to my BlackBerry," he told CNBC in January 2009, days before his inauguration.

The Obama transition team produced a military-grade phone without a microphone, camera, or location tracker that could not make or receive calls.

"I get the thing, and they're all like, 'Well, Mr. President, for security reasons ... it doesn't take pictures, you can't text, the phone doesn't work ... you can't play your music on it,'" Obama told Jimmy Fallon in 2016. "Basically, it's like, does your 3-year-old have one of those play phones?"

*Eric Geller contributed to to this report.*

LILY HAY NEWMAN SECURITY 06.15.18 04:11 PM

# TRUMP SAYS HE GAVE KIM JONG UN HIS DIRECT NUMBER. NEVER DO THAT

SAUL LOEB/AFP/GETTY IMAGES

**DAYS AFTER PRESIDENT** Donald Trump met with North Korean dictator Kim Jong Un in Singapore, the president touted the strength of the two leaders' relationship. "I can now call him," he told reporters at the White House on Friday. "I gave him a very direct number. He can now call me if he has any difficulty. We have communication."

The US and North Korea have an extremely complicated and thorny diplomatic relationship—it wasn't long ago that Trump casually threatened a nuclear strike—and any gesture of goodwill between the two nations potentially helps better it. But Trump's claim concerned security experts Friday, who noted that if the president really did give his personal number to Kim Jong Un, he would also have created a major national security exposure in the process.

"Absolutely that is a problem," says Karsten Nohl, chief scientist at the German firm Security Research Labs, who researches cell network attacks. Hackers can abuse flaws in the way cellphone networks interoperate to listen in on someone's phone calls, intercept their text messages, and track their location. If

tool for spying on the top tier of the US government. The White House did not return a request for comment.

"If he were well-advised and listened to that advice, he would probably give out a random phone number that forwards to his phone number, versus a phone number that is really off of the SIM card in his phone," Nohl says. "As president of the US, he could probably have a list of 1,000 phone numbers, all of which reach his phone."

That's how things are supposed to work. But Trump has a poor track record for maintaining cyberhygiene within the White House. He brought his personal Android phone there when he first began his presidency, and has shown reported reluctance to turn his government-issued smartphones in to the White House IT department for scanning or to be swapped out.

"I wouldn't be surprised if everybody has malware on Trump's smartphones," says Dave Aitel, a former NSA researcher who now runs the penetration testing firm Immunity.

Furthermore, a CNN report from late April indicated that Trump has recently *increased* his personal smartphone use, including for conversations with GOP lawmakers, partly in an effort to circumvent the White House switchboard altogether.

All told, you have a situation in which the President of the United States uses a likely insecure smartphone, coupled with at least the possibility that he has given the number of that smartphone to the leader of a hostile foreign power that loves to hack. "It's definitely not the perfect scenario," Nohl says.

If North Korean intelligence isn't already tracking Trump's phones through malware, a direct phone number could give them a way in. The main type of known cell network exploits, called SS7 attacks, can give hackers relatively easy access to calls and texts, not to mention location data. The FCC has been

working on broader fixes for the vulnerabilities, and the threat isn't just hypothetical. The Department of Homeland Security acknowledged at the end of May that hackers may have used SS7 attacks against US cellphone users.

Because SS7 attacks involve manipulating connections between different cell networks—and carriers keep records of those connections—they can be spotted, especially against a number as high-value as Trump's. That doesn't mean a hacker couldn't strategically use the attacks once or twice, though, choosing to burn their advantage at a calculated moment. Nohl also points out that it would be more difficult to watch for signs of an SS7 attack when Trump is traveling abroad and on foreign carriers, if he brings and uses his smartphones while traveling and the devices are allowed to roam.

North Korea has proven itself as an adversary willing to hack and manipulate systems around the world for its financial or intelligence gain—it was responsible both for the devastating hack of Sony in 2014 and last year's WannaCry ransomware meltdown—and SS7 hacking is likely no exception. The global community has struggled to manage North Korean hackers, though, since they are particularly brazen and shameless. If the US caught North Korea spying on Trump's phone, it would be difficult to select an appropriate deterrent response.

The White House is certainly equipped for secure calling, and hopefully Trump followed protocols such that his late-night gabfests with Kim Jong Un happen on a secure line and can focus on friendship and fun. But if Trump gave the reclusive dictator the access he claims, that recklessness could become a problem.

## More Great WIRED Stories

- The hustlers fueling cryptocurrency's marketing machine
- This elite Microsoft hacker team keeps Windows PCs safe
- The brilliant vigilance of Seattle's gargantuan new tunnel