



# Department of Justice

---

**STATEMENT OF**

**CHRISTOPHER A. WRAY  
DIRECTOR  
FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE  
COMMITTEE ON HOMELAND SECURITY  
U.S. HOUSE OF REPRESENTATIVES**

**AT A HEARING ENTITLED  
“WORLDWIDE THREATS”**

**PRESENTED  
SEPTEMBER 22, 2021**

**STATEMENT OF  
CHRISTOPHER A. WRAY  
DIRECTOR  
FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE  
COMMITTEE ON HOMELAND SECURITY  
U.S. HOUSE OF REPRESENTATIVES**

**AT A HEARING ENTITLED  
“WORLDWIDE THREATS”**

**PRESENTED  
SEPTEMBER 22, 2021**

---

Good morning, Chairman Thompson, Ranking Member Katko, and Members of the Committee. Thank you for inviting me here today to discuss the threats facing our homeland. A week and a half ago, we marked a somber anniversary in this country — 20 years since the September 11<sup>th</sup> attacks.

September 11th represents evil and loss. But it also represents sacrifice and selflessness. It represents grit and resilience and strength in the face of great adversity. And two decades later, it has come to represent the FBI’s continued ability to adapt to a changing world, and to stay laser focused on keeping our country safe from another attack like that one.

About two years after the 9/11 attacks, when I was the Assistant Attorney General overseeing the Justice Department’s terrorism portfolio, I had the chance to meet with members of the victims’ families. Those families and their stories left an impression that I’ll never forget. The kind of knee-buckling grief those families experienced — that sense that something you held most precious was stolen from you — never goes away.

Of course, we can’t think of 9/11 without recalling the sacrifices made on that day and the days after. We continue to honor members of the FBI family who died that day; our FBI brothers and sisters who have since lost their lives to illnesses resulting from their work after the attacks; and those fighting grave illnesses today. These selfless men and women thought of others first and answered the call of duty, no matter the cost.

I would like to talk a bit about how the FBI has transformed in the past two decades, and how the threats we face today have evolved during that time.

## **FBI Transformation**

Twenty years ago, I was working in senior leadership at the Department of Justice. On the afternoon of September 11<sup>th</sup>, 2001, I was at FBI Headquarters, in the Strategic Information and Operations Center, with Director Mueller and Attorney General Ashcroft. Although it was a chaotic, horrifying time, it was also a time of incredible solidarity. Everyone there that day had one purpose, and that was to make sure that what we had just experienced as a nation would never, ever happen again.

For a long time, we lived in a haze that seemed like September 12<sup>th</sup>, day after day after day. Every lead, every tip, every threat seemed like it could be the next one. We kept asking ourselves, “What could we have done better? What should we have done better?” And now every day, we wake up asking ourselves, “What do we need to do to keep people safe today... and tomorrow ... and the day after that?”

Under Director Mueller’s leadership, the FBI made a paradigm shift, dramatically expanding national security operations, and changing the way we did business: shifting to focus intently on disrupting attacks before they occur and on working with and through our partners around the world and at every level of government here at home. When I left the Department of Justice in 2005, those changes were still in their infancy. When I take stock of where things stand now, all these years later, I am astounded by the progress.

It is incredible to see firsthand the capabilities we have built with our partners here and around the world. Today we are all stronger, smarter, and better able to confront the threats we face.

Preventing terrorist attacks, from any place, by any actor, remains the FBI’s top priority. The nature of the threat posed by terrorism — both international terrorism (“IT”) and domestic terrorism (“DT”) — continues to evolve.

To meet that evolving threat, the FBI has surged resources to our domestic terrorism investigations in the last year, increasing personnel by 260 percent. Importantly, however, our increased focus on domestic terrorism is not at the expense of our work on other terrorism threats. We continue to monitor potential threats by foreign terrorist organizations like al Qaeda and ISIS, which have never stopped expressing their intent to carry out large-scale attacks like 9/11 here in the United States. And we are also monitoring other dangerous groups like Iran’s Islamic Revolutionary Guard Corps.

Of course, in addition to terrorism threats, we also face a wide array of cyber threats from nation state and criminal actors alike; persistent counterintelligence threats from the People’s Republic of China (“P.R.C.”), Russia, Iran, and North Korea; and the full spectrum of criminal threats, from hate crimes and other civil rights abuses to violent crime spikes in cities across this country, to human trafficking and crimes against children, just to name a few.

But no matter which threats have dominated the landscape over the last 20 years, the FBI has remained focused on prevention and disruption – sharing intelligence and making arrests before criminals and terrorists can act. And we have remained focused on our ultimate mission: protecting the American people and upholding the Constitution.

## **Capitol Violence**

First and foremost, I want to assure you, your staff, and the American people that the FBI has deployed our full investigative resources and is working closely with our federal, State, local, Tribal, and territorial partners to aggressively pursue those involved in criminal activity during the events of January 6, 2021. We are working hard to identify those responsible for the violence and destruction of property at the U.S. Capitol building.

FBI Special Agents, Intelligence Analysts, and professional staff have been hard at work gathering evidence, sharing intelligence, and working with federal prosecutors to bring charges against the individuals involved. As we have said consistently, we do not and will not tolerate violent extremists who use the guise of First Amendment-protected activity to engage in violent criminal activity. Thus far, the FBI has arrested hundreds of individuals with regards to rioting, assault on a federal officer, property crimes violations, and conspiracy charges, and the work continues.

Overall, the FBI assesses that the January 6<sup>th</sup> siege of the Capitol Complex demonstrates a willingness by some to use violence against the government in furtherance of their political and social goals. This ideologically motivated violence — domestic terrorism — underscores the symbolic nature of the National Capital Region and the willingness of some Domestic Violent Extremists to travel to events in this area and violently engage law enforcement and their perceived adversaries. The American people should rest assured that we will continue to work to hold accountable those individuals who participated in the violent breach of the Capitol on January 6<sup>th</sup> and any others who attempt to use violence to intimidate, coerce, or influence the American people or affect the conduct of our government.

## **Top Terrorism Threats**

There are some commonalities between the IT and DT threats, most importantly the danger posed by lone actors or small cells who typically radicalize online and look to attack soft targets with easily accessible weapons. Individuals who commit violent criminal acts in furtherance of social or political goals stemming from domestic influences — some of which include racial or ethnic bias, or anti-government or anti-authority sentiments — are described as Domestic Violent Extremists (“DVEs”), whereas individuals who are inspired primarily by global jihad but are not receiving individualized direction from Foreign Terrorist Organizations (“FTOs”) are known as Homegrown Violent Extremists (“HVEs”). Both of these threats, which together form the most significant terrorism danger to our country, are located primarily in the United States and typically radicalize and mobilize to violence on their own.

DVEs and HVEs are often motivated and inspired by a mix of socio-political, ideological, and personal grievances against their targets, and more recently have focused on accessible targets including civilians, houses of worship, retail locations, and mass public gatherings. Selecting these types of soft targets, in addition to the insular nature of their radicalization and mobilization to violence and limited discussions with others regarding their plans, increases the challenge faced by law enforcement to detect and disrupt the activities of lone actors before they occur. Some violent extremists have also continued to target law enforcement and the military as well as symbols or members of the U.S. Government.

The top threats we face from DVEs are from those we categorize as Racially or Ethnically Motivated Violent Extremists (“RMVEs”) and Anti-Government or Anti-Authority Violent Extremists. While RMVEs who advocate for the superiority of the white race were the primary source of lethal attacks perpetrated by DVEs in 2018 and 2019, Anti-Government or Anti-Authority Violent Extremists – specifically, Militia Violent Extremists and Anarchist Violent Extremists – were responsible for three of the four lethal DVE attacks in 2020. Notably, this included the first lethal attack committed by an Anarchist Violent Extremist in over 20 years.

Consistent with our mission, the FBI holds sacred the rights of individuals to peacefully exercise their First Amendment freedoms. Regardless of their specific ideology, the FBI will aggressively pursue those who seek to hijack legitimate First Amendment-protected activity by engaging in violent criminal activity such as the destruction of property and violent assaults on law enforcement officers that we witnessed on January 6<sup>th</sup> and during protests throughout the United States during the summer of 2020. The FBI will actively pursue the opening of FBI investigations when an individual uses — or threatens the use of — force, violence, or coercion, in violation of federal law and in the furtherance of social or political goals.

The FBI assesses that HVEs pose the greatest, most immediate IT threat to the Homeland. They typically are not receiving individualized direction from global jihad-inspired FTOs but are inspired largely by the Islamic State of Iraq and ash-Sham (“ISIS”) and al-Qa’ida to commit violence. HVEs’ lack of a direct connection to an FTO, their ability to rapidly mobilize without detection, and their use of encrypted communications pose significant challenges to our ability to proactively identify and disrupt them.

The FBI remains concerned that FTOs, such as ISIS and al-Qa’ida, intend to carry out or inspire large-scale attacks in the United States. As we saw in the murder in Kabul last month of 13 brave American service men and women and nearly 200 Afghans, ISIS remains relentless in its campaign of violence against the United States and our partners — both here at home and overseas. To this day, ISIS continues to aggressively promote its hate-fueled rhetoric and attract like-minded violent extremists with a willingness to conduct attacks against the United States and our interests abroad. ISIS’ successful use of social media and messaging applications to attract individuals seeking a sense of belonging is of continued concern to us. Like other foreign terrorist groups, ISIS advocates for lone offender attacks in the United States and Western countries via videos and other English language propaganda that have at times

specifically advocated for attacks against civilians, the military, law enforcement and other government personnel.

Al-Qa'ida maintains its desire to both conduct and inspire large-scale, spectacular attacks. Because continued pressure has degraded some of the group's senior leadership, in the near term, we assess that al-Qa'ida is more likely to continue to focus on cultivating its international affiliates and supporting small-scale, readily achievable attacks, including attacks against the interests of the United States and other Western nations, in regions such as East and West Africa. Over the past year, propaganda from al-Qa'ida leaders continued to seek to inspire individuals to conduct attacks in the United States and other Western nations. We expect those attempts to continue.

Iran and its global proxies and partners, including Iraqi Shia militant groups, continue to attack and plot against the United States and our allies throughout the Middle East in response to U.S. pressure. Iran's Islamic Revolutionary Guard Corps-Qods Force ("IRGC-QF") continues to provide support to militant resistance groups and terrorist organizations. Lebanese Hizballah, Iran's primary strategic partner, has sent operatives to build terrorist infrastructures worldwide. Hizballah also continues to conduct intelligence collection, financial activities, and procurement efforts worldwide to support its terrorist capabilities. FBI arrests in recent years of alleged Iranian and Hizballah operatives in the United States suggest the Government of Iran and Hizballah each seek to establish infrastructure here, potentially for the purpose of conducting operational or contingency planning. IRGC-QF Commander Esmail Ghani and Hizballah Secretary General Hasan Nasrallah have each threatened retaliation for the death of IRGC-QF Commander Qassem Soleimani.

As an organization, we continually adapt and rely heavily on the strength of our federal, State, local, Tribal, territorial, and international partnerships to combat all terrorist threats to the United States and our interests. To that end, we use all available lawful investigative techniques and methods to combat these threats while continuing to collect, analyze, and share intelligence concerning the threat posed by violent extremists, in all their forms, who desire to harm Americans and U.S. interests. We will continue to share information and encourage the sharing of information among our numerous partners via our Joint Terrorism Task Forces across the country, and our Legal Attaché offices around the world.

## **Cyber**

In the last decade, while professionals toiled against a steady drumbeat of malicious cyber activities, typically only one or two major cyber incidents captured the nation's attention each year: the Sony Pictures hack in 2014, the announcement of the OPM data breach incident in 2015, Russian election interference in 2016, and the WannaCry ransomware and NotPetya attacks of 2017. This past year, a steady stream of high-profile cyber incidents has garnered worldwide attention, beginning with the SolarWinds incident at the very end of 2020; followed by the Microsoft Exchange Server intrusions revealed in March; significant exploitation of Pulse Secure vulnerabilities in April; and then ransomware attacks against Colonial Pipeline,

JBS USA, and customers of Kaseya between May and July, among thousands of other incidents targeting victims in the U.S. and worldwide.

Throughout the last year, the FBI has seen a wider-than-ever range of cyber actors threaten Americans' safety, security, and confidence in our digitally connected world. Cyber-criminal syndicates and nation-states keep innovating to compromise our networks and maximize the reach and impact of their operations, such as by selling malware as a service or by targeting vendors to access scores of victims by hacking just one provider.

With each significant cyber incident, our surge to the affected victim serves a host of purposes at once. The evidence and intelligence we develop helps that victim effectively detect and remediate the intrusion; identifies other victims and potential future targets of the same actors that we can notify and work with our partners to assist; and develops the attribution to and knowledge of the adversary that we as a government need to effectively respond. When other incident responders leave the scene, our work to analyze the evidence, identify those responsible, and hold them accountable can continue for months, even years. In the SolarWinds investigation, just one field office collected more than 170 terabytes of data — that's 17 times the content housed within the Library of Congress in one office for one investigation. We bought tens of thousands of dollars of new servers just to house the data, but that doesn't begin to take into account the time and talent it takes to exploit it, share it, and act upon it.

The situation is not sustainable, and it's not acceptable. Cyber criminals and nation states believe that they can compromise our networks, steal our property, and hold our critical infrastructure at risk without incurring any risk themselves. In the last year alone, we have seen — and have publicly called out — the P.R.C., North Korea, and Russia for using cyber operations to target U.S. COVID-19 vaccines and research. We have seen the far-reaching disruptive impact a serious supply-chain compromise can have through the SolarWinds intrusions, conducted by the Russian SVR. We have seen the P.R.C. working to obtain controlled defense technology and developing the ability to use cyber means to complement any future real-world conflict. We also recently unsealed an indictment against four P.R.C. Nationals working with the Ministry of State Security. The four individuals were charged with a campaign to hack into the computer systems of dozens of victims while trying to obtain information with significant economic benefit to the P.R.C. Iran used cyber means to try to sow divisions and undermine our elections, targeting voters before the November election, and threatening election officials after. North Korea's cyber capabilities have increased in recent years, posing a particular threat to financial institutions and a growing cyber espionage threat.

As dangerous as nation-states are, we do not have the luxury of focusing on them alone. Ransomware has always been treated by the FBI as a serious cybercriminal threat. But as the President has observed, ransomware has evolved into a national security issue, affecting the critical infrastructure we can least afford to be without. Last year, there was a 20% increase in the number of ransomware incidents reported to the FBI's Internet Crime Complaint Center and a 225% increase in ransom amounts. Unfortunately, ransomware incidents are not only becoming more common, but also more dangerous. Ransomware incidents in the past year have

hit victims in nearly every critical infrastructure sector. While attacks against Colonial Pipeline and JBS USA made national headlines, ransomware actors have also targeted hospitals and medical centers, putting patients' lives at an increased risk at a time when America faces its most dire public health crisis in generations. While we are bringing our unique dual criminal and national security authorities to the fight, we recognize that we cannot fully combat this threat without international cooperation. We have been working with our partners in the State Department and the National Security Council to increase pressure on countries that consistently fail to take action to stop ransomware actors in their territory, particularly Russia. We will continue to tackle the ransomware threat through a whole-of-government approach, but we also need foreign nations to do their part to keep cybercriminals from acting with impunity within their borders.

Dark web vendors who sell capabilities in exchange for cryptocurrency are making it more difficult for us to stop what would once have been less dangerous offenders. Although once a ring of relatively unsophisticated criminals, these actors are now armed with the tools to paralyze entire hospitals, police departments, and businesses with ransomware. It is not that individual hackers alone have necessarily become much more sophisticated, but — unlike previously — they are able to rent sophisticated capabilities.

We have to make it harder and more painful for hackers to steal our intellectual property and hold our networks at risk. That is why I announced a new FBI cyber strategy last year, using the FBI's role as the lead federal agency with law enforcement and intelligence responsibilities to not only pursue our own disruptive actions, but to work seamlessly with our domestic and international partners to defend networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries overseas.

FBI's strategy of using our information to enable our partners has been successful in taking down cyber criminal enterprises. Each success has this in common: multiple U.S. agencies working — often with multiple international partners — to bring our information and tools together to achieve the most significant, durable impact. One example of this approach is the international takedown in January 2021 of the Emotet botnet, which enabled a network of cyber criminals to cause hundreds of millions of dollars in damages to government, educational, and corporate networks. The FBI used sophisticated techniques, our unique legal authorities, and, most importantly, our worldwide partnerships to significantly disrupt the malware, working with an unprecedented number of international law enforcement agencies.

Also this January, we worked with Canada and Bulgaria to disrupt NetWalker, a ransomware variant that paralyzed companies, municipalities, hospitals, law enforcement agencies, emergency services, school districts, colleges, and universities. We obtained federal charges, seized more than \$450,000 in cryptocurrency, and the United States requested Canada's arrest of a subject who is facing extradition proceedings.

Our joint efforts extend to our partners in private industry, especially those providers that have unique visibility into how adversaries are exploiting U.S. networks. In March,

cybersecurity companies including Microsoft disclosed that hackers — who have since been identified as affiliated with the P.R.C.’s Ministry of State Security — were using previously unknown Microsoft Exchange vulnerabilities to access email servers that companies physically keep on their premises rather than in the cloud. These “zero day” vulnerabilities allowed the P.R.C. actors to potentially exploit victim networks such as by grabbing login credentials, stealing email messages in bulk, and installing malicious programs (“web shells”) allowing the hackers to send commands to the victim network. First, the FBI put out a joint advisory with the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (“CISA”) to give network defenders the technical information they needed to mitigate the vulnerability. However, while many infected system owners successfully removed the web shells, others were not able to do so. That left many systems vulnerable to Chinese cyber actors who could continue to steal information, or potentially even execute a destructive attack.

We thought that risk was unacceptable, especially when it was within our authorities to do something about it. So, we used those authorities, through a court-authorized operation in partnership with the private sector, to remove malicious web shells from hundreds of vulnerable computers in the U.S. running Microsoft Exchange Server software. The P.R.C. propped open backdoors throughout U.S. networks. We slammed them shut.

These are the incidents that garner the most attention, but behind the scenes the FBI took upwards of 1,100 actions against cyber adversaries last year, including arrests, criminal charges, convictions, dismantlements, and disruptions; and enabled many more actions through our dedicated partnerships with the private sector, foreign partners, and at the federal, State, and local level. In some instances, we were also able to seize cybercriminals’ ill-gotten gains, with the most publicized example being the seizure of \$2.3 million in cryptocurrency paid to the DarkSide ransomware group that targeted Colonial Pipeline.

We have been putting a lot of energy and resources into all of those partnerships, especially with the private sector. We are working hard to push important threat information to network defenders, while also been making it as easy as possible for the private sector to share important information with us. We emphasize how we keep our presence unobtrusive in the wake of a breach, how we protect information that the private sector shares with us and commit to providing useful information back, and how we coordinate with our government partners so that we are speaking with one voice.

But we need the private sector to do its part, too. We need the private sector to come forward to warn us quickly when they see malicious cyber activity. We also need the private sector to work with us when we warn them that they are being targeted. The recent examples of significant cyber incidents only emphasize what I have been saying for a long time: The government cannot protect against cyber threats on its own. We need a whole-of-society approach that matches the scope of the danger. We wholeheartedly support the Administration’s view that legislation is needed to require reporting of significant cyber incidents, including ransomware attacks, cyber incidents that affect critical infrastructure entities, and other incidents that implicate heightened risks to the government, the public, or

third parties. There is really no other option for defending a country where the vast majority of our critical infrastructure, personal data, intellectual property, and network infrastructure sits in private hands.

## **Foreign Malign Influence**

Our nation is confronting multifaceted foreign threats seeking to both influence our national policies and public opinion, and cause harm to our national dialogue. The FBI and our interagency partners remain concerned about, and focused on, malign influence measures used by certain adversaries in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes.

Foreign malign influence operations — which include subversive, undeclared, coercive, and criminal actions by foreign governments to influence U.S. political sentiment or public discourse or interfere in our democratic processes themselves — are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. Foreign malign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries — hoping to reach a wide swath of Americans covertly from outside the United States — to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.

The FBI is the lead federal agency responsible for investigating foreign malign influence operations. In the fall of 2017, we established the Foreign Influence Task Force (“FITF”) to identify and counteract malign foreign influence operations targeting the United States. The FITF is led by the Counterintelligence Division and is comprised of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign malign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions; develop a common understanding of threats with our interagency partners; raise adversaries' costs; and disrupt foreign malign influence operations and enablers in the United States and worldwide.

While we are keenly focused on threats to elections, those events are not the only aspects of our democracy that are being threatened. Our adversaries are also targeting the very fabric of our civil discourse and are targeting policy processes at every level of government — State, local and federal. The FITF brings the FBI's national security and traditional criminal investigative expertise under one umbrella to better understand and combat these complex and nuanced threats. This cross-programmatic approach allows the FBI to identify connections across programs, to aggressively investigate as appropriate, and — importantly — to be more agile. Coordinating closely with our partners and leveraging relationships we have developed in

the technology sector, we regularly relay threat indicators that those companies use to take swift action, blocking budding abuse of their platforms.

Following the 2018 midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat foreign malign influence focused solely on the threat posed by Russia. Using lessons learned from the 2018 mid-term elections, the FITF widened its aperture to confront foreign malign operations of the P.R.C., Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent coverage of foreign malign influence threats, including threats to our elections.

These additional resources were also devoted to working with U.S. Government partners on two documents regarding the U.S. Government's analysis of foreign efforts to influence or interfere with the 2020 Election. The reports are separate but complementary and were published earlier this year. The first report — referred to as the 1a report and authored by the Office of the Director of National Intelligence — outlines the intentions of foreign adversaries with regard to influencing and interfering with the election but does not evaluate impact. The second report — referred to as the 1b report and authored by the Department of Justice, including the FBI, and Department of Homeland Security, including CISA — evaluates the impact of foreign government activity on the security or integrity of election infrastructure or infrastructure pertaining to political organizations, candidates, or campaigns.

The main takeaway from both reports is that there is no evidence — not through intelligence collection on the foreign actors themselves, not through physical security and cybersecurity monitoring of voting systems across the country, not through post-election audits, and not through any other means — that a foreign government or other actors compromised election infrastructure to manipulate election results.

Another way in which foreign governments reach across borders to influence and target diaspora communities in the United States is through “transnational repression,” which is the growing practice of governments silencing exiles and members of diasporas — including activists, dissidents, defectors, journalists, and other critics — living outside of their territorial borders. Iran, the P.R.C., and other authoritarian regimes continue to target dissidents and human rights activists on U.S. soil. The Administration is committed to addressing this challenge as part of our broader commitment to stem rising authoritarianism.

We remain vigilant in understanding and combating foreign malign influence in the homeland and look across the U.S. Government — in our intelligence community partners and beyond — as we work to effectively protect our elections, democratic processes, and the American people.

## Lawful Access

The problems caused by law enforcement agencies' inability to access electronic evidence continue to grow. Increasingly, commercial device manufacturers have employed encryption in such a manner that only the device users can access the content of the devices. This is commonly referred to as "user-only-access" device encryption. Similarly, more and more communications service providers are designing their platforms and apps such that only the parties to the communication can access the content. This is generally known as "end-to-end" encryption. The proliferation of end-to-end and user-only-access encryption is a serious issue that increasingly limits law enforcement's ability, even after obtaining a lawful warrant or court order, to access critical evidence and information needed to disrupt threats, protect the public, and bring perpetrators to justice.

The FBI remains a strong advocate for the wide and consistent use of responsibly-managed encryption — encryption that providers can decrypt and provide to law enforcement when served with a legal order. Protecting data and privacy in a digitally connected world is a top priority for the FBI and we believe that promoting encryption is a vital part of that mission. But we have seen that the broad application of end-to-end and user-only-access encryption adds negligible security advantages. It does have a negative effect on law enforcement's ability to protect the public. What we mean when we talk about lawful access is putting providers who manage encrypted data in a position to decrypt it and provide it to us in response to legal process. We are not asking for, and do not want, any "backdoor," that is, for encryption to be weakened or compromised so that it can be defeated from the outside by law enforcement or anyone else. Unfortunately, too much of the debate over lawful access has revolved around discussions of this "backdoor" straw man instead of what we really want and need.

We are deeply concerned about the threat that end-to-end and user-only-access encryption pose to our ability to fulfill the FBI's duty of protecting the American people from every manner of federal crime, from cyber-attacks and violence against children to drug trafficking and organized crime. We believe Americans deserve security in every walk of life — in their data, their streets, their businesses, and their communities.

End-to-end and user-only-access encryption erode that security against every danger the FBI combats. For example, even with our substantial resources, accessing the content of known or suspected terrorists' data pursuant to court-authorized legal process is increasingly difficult. The often-online nature of the terrorist radicalization process, along with the insular nature of most of today's attack plotters, leaves fewer dots for investigators to connect in time to stop an attack, and end-to-end and user-only-access encryption increasingly hide even those often precious few and fleeting dots.

In one instance, while planning — and right up until the eve of — the December 6, 2019, shooting at Naval Air Station Pensacola that killed three U.S. sailors and severely wounded eight other Americans, deceased terrorist Mohammed Saeed Al-Shamrani communicated undetected with overseas al-Qa'ida terrorists using an end-to-end encrypted app.

Then, after the attack, user-only-access encryption prevented the FBI from accessing information contained in his phones for several months. As a result, during the critical time period immediately following the shooting and despite obtaining search warrants for the deceased killer's devices, the FBI could not access the information on those phones to identify co-conspirators or determine whether they may have been plotting additional attacks.

This problem spans international and domestic terrorism threats. Like Al-Shamrani, the plotters who sought to kidnap the Governor of Michigan late last year used end-to-end encrypted apps to hide their communications from law enforcement. Their plot was disrupted only by well-timed human source reporting and the resulting undercover operation. Subjects of our investigation into the January 6<sup>th</sup> Capitol siege used end-to-end encrypted communications as well.

We face the same problem in protecting children against violent sexual exploitation. End-to-end and user-only-access encryption frequently prevent us from discovering and searching for victims, since the vital tips we receive from providers only arrive when those providers themselves are able to detect and report child exploitation being facilitated on their platforms and services. They cannot do that when their platforms are end-to-end encrypted. For example, while Facebook Messenger and Apple iMessage each boasts over one billion users, in 2020, the National Center for Missing and Exploited Children ("NCMEC") received over 20 million tips from Facebook<sup>1</sup>, compared to 265 tips from Apple, according to NCMEC data and publicly available information. Apple's use of end-to-end encryption, which blinds it to child sexual abuse material being transmitted through its services, likely plays a role in the disparities in reporting between the two companies. We do not know how many children are being harmed across the country as a result of this under-reporting by Apple and other end-to-end providers.<sup>2</sup>

When we are able to open investigations, end-to-end and user-only-access encryption makes it much more difficult to bring perpetrators to justice. Much evidence of crimes against children, just like the evidence of many other kinds of crime today, exists primarily in electronic form. If we cannot obtain that critical electronic evidence, our efforts are frequently hamstrung.

This problem is not just limited to federal investigations. Our State and local law enforcement partners have been consistently advising the FBI that they, too, are experiencing similar end-to-end and user-only-access encryption challenges, which are now being felt across the full range of State and local criminal law enforcement. Many report that even relatively unsophisticated criminal groups, like street gangs, are frequently using user-only-access encrypted smartphones and end-to-end encrypted communications apps to shield their activities from detection or disruption. As this problem becomes more and more acute for State and local

---

<sup>1</sup>Facebook is planning to move its Facebook Messenger platform to end-to-end encryption as a default in the near future. This will result in the loss of even these tips.

<sup>2</sup>In light of the ongoing harm caused by under-reporting of abuse, it is important for companies attempting to improve reporting to follow through in a timely manner.

law enforcement, the advanced technical resources needed to address even a single investigation involving end-to-end and user-only-access encryption will continue to diminish and ultimately the capacity of State and local law enforcement to investigate even common crimes will be overwhelmed.

## **Conclusion**

The threats we face as a nation have never been greater or more diverse, and the expectations placed on the FBI have never been higher. Our fellow citizens look to the FBI to protect the United States from all of those threats, and the men and women of the FBI continue to meet and exceed those expectations, every day. I want to thank them for their dedicated service.

Chairman Thompson, Ranking Member Katko, and Members of the Committee, thank you for the opportunity to testify today. I am happy to answer any questions you might have.