Darrin Jones, FBI; President's Commission on Law Enforcement and the Administration of Justice; Crime Reduction Hearing, April 15, 2020.

Good afternoon Chairman Keith, Vice Chair Sullivan, commissioners and distinguished guests. Thank you for inviting me to testify today.

My name is Darrin Jones, I am the Executive Assistant Director for the Science and Technology Branch at the FBI. It is from within this branch that the FBI effectuates federal court orders for the interception of communications and assists our field offices in accessing a wide range of digital evidence. I've had a front row seat to witness the steady erosion of Law Enforcement's ability to access electronic evidence and conduct court authorized electronic surveillance.

Over the last decade, a number of major US tech companies have chosen to independently design, develop, and then implement certain forms of technology, in this case increasingly complex, user-controlled encryption, ostensibly, in ways that no one other than the users can readily or timely access the contents of communications or other stored data. As is well known, this results in the creation of "lawless spaces" on the internet where law enforcement, even when armed with a Constitutionally-sound search warrant or wiretap order, are incapable of readily penetrating. These "lawless spaces" represent an ever-expanding universe of illegal and illicit activity, which threatens the lives and safety of our children, our economy, our national security, and even our elections.

In addition to my position at the FBI, I also currently serve as co-chair of the Commission's Technology Working Group. On behalf of that working group I would share the following recommendation:

> **Federal legislation must be enacted to compel major technology companies to design for themselves strong encryption regimes for their products and services that protect privacy but that permit lawful access pursuant to the due process of law.**

Darrin Jones, FBI; President's Commission on Law Enforcement and the Administration of Justice; Crime Reduction Hearing, April 15, 2020.

That language may sound familiar to many of you. The working group decided to mirror the language adopted by resolution in December 2019 by more than 30,000 IACP members representing over 160 countries.

For more than 200 years our Constitution, the Fourth Amendment, and our courts have balanced our privacy and the need for law enforcement to have access to the evidence society need to stop criminals, pursue justice for victims, and protect its citizens. Why should it be different in the digital world? We now find ourselves in a place where not the courts, but individual companies are deciding what's of greatest importance for all of us. Put another way, we're allowing technology to dictate our national core values rather than ensuring our national core values drive how we implement technology.

It has now been 131 days since a foreign terrorist in Pensacola, Florida, murdered in cold blood, three US service members on a US military base. Then, before being killed in a shootout with law enforcement, the terrorist took the time to put a bullet in his phone in a clear attempt to destroy it and all evidence it contained. We are still trying to access that phone. That's what I mean when I say we have a "lawful access" problem.

In a recent Gang Task Force case, source reporting and traditional telephony intercepts indicated that the main subject, suspected of ordering the homicide of another drug dealer, was using Facetime to discuss and coordinate criminal activity with his co-conspirators. Indeed, he frequently directed them to use FaceTime instead of traditional cellular telephones because FaceTime, a product of Apple uses, end-to-end encryption. Investigators, realizing they would not recover the content of FaceTime communications, did not pursue legal process. Post-arrest statements by the subjects confirmed they were well aware that those **not** arrested were only those co-conspirators exclusively using encrypted communications. That's what I mean when I say Law Enforcement has a "lawful access" problem.

Similarly, a recent OCDETF (Organized Crime Drug Enforcement Task Force) case indicated multiple subjects responsible for illicitly transporting large quantities of heroin, methamphetamine, cocaine and marijuana from the southern border to the Great Lakes region for further distribution regularly used encrypted apps to evade law enforcement detection. Senior members of the drug trafficking organization routinely instructed underlings to use WhatsApp, Telegram or Snapchat. Communications that would go unanswered on traditional cellular telephones were immediately accepted and responded to using encrypted Apps. Due to the inability to obtain content, OCDETF investigators did not pursue a Title III order. That's what I mean when I say we have a "lawful access" problem.

As most of you are aware, Mr. Zuckerberg has announced that he intends to encrypt FB Messenger soon. What that means is, one man has independently decided to implement technology, in this case end-to-end encryption, in such a way that even if a judge issues a warrant, no one, including law enforcement, can access those messages. In 2019 Facebook's platforms, primarily Facebook Messenger, sent over 15M tips to the National Center for Missing and Exploited Children. NCMEC immediately forwarded those tips to state and local law enforcement agencies across the country. They took them to judges, who issued warrants, which allowed those agencies to rescue thousands of kids. One man, one company is independently deciding whether or not that should continue.

The ubiquity of end-to-end encryption and other user-only access encryption products and applications causes them to be encountered nearly daily by state and local police departments. The impact of this challenge not only means an increase in unsolvable crimes and a denial of justice for victims, but also threatens to dramatically alter the nation's dual-sovereign federal system of law enforcement. Let me tell you how, because this may not be intuitive. When local police departments are without resources to timely and cost-effectively gain lawful access to critical criminal evidence that has been encrypted, they will necessarily have to turn to larger federal agencies such as the FBI for assistance. Under such a paradigm, the foreseeable result

may be that a federal agency may reluctantly but practicably find itself in the position of effectively dictating which state and local crimes are investigated and prosecuted regardless of the priorities of state and local officials. State and local agencies must maintain lawful access to electronic evidence in order to retain their basic jurisdictional sovereignty and to ensure that enforcement of local crimes is controlled at the local level.

In response, a number of major tech companies and academics have publicly proffered a solution to the lawful access challenge which is arguably as inappropriate as it is disingenuous: namely, that law enforcement should develop better hacking skills to keep pace with industry products, even though these same companies freely admit that they would quickly work to block any exploit used by law enforcement to gain access in execution of a court order. The prospect of police departments, which are already confronting major traditional crime-fighting personnel and resource challenges, entering into what would, in essence, be a cryptologic arms race with Apple or Google is not only ludicrous, but it confirms the existence of an industry mindset which believes that it controls this public policy debate in place of democratically-elected governments.

The tech companies would have you believe that it's impossible to allow lawful access while maintaining strong cyber security. In response, Bill Gates, founder of Microsoft, has said, "[T]he companies need to be careful that they're not ... advocating things that would prevent government from being able to, under appropriate review, perform the type of functions that we've come to count on." When asked if he was referring to iPhone unlocking, Gates suggested: "There's no question of ability; it's the question of willingness." Butler Lampson—a winner of the Turing Award, the Nobel Prize of computer science—calls the approach "completely reasonable … The idea that there's no way to engineer a secure way of access is ridiculous."

Darrin Jones, FBI; President's Commission on Law Enforcement and the Administration of Justice; Crime Reduction Hearing, April 15, 2020.

I feel like I need to add that I am always personally stunned when I hear companies talking about law enforcement trying to build a "back door." We're not trying to build a "back door," to anything – we're asking companies to be able to open the door when law enforcement has a lawful court-authorized search warrant. What they're trying to do is block the door – build the door and barricade it – and prevent it from being opened by law enforcement, for any reason. They seem to be okay with using encryption to prevent law enforcement from opening the door and accessing the house whether or not there is a spy hiding behind the door, a terrorist behind the door who killed our sailors on a military base in our own country, an MS-13 member preparing to kill again, or a kidnapped child behind the door who needs to be rescued. They're openly telling us they're going to bar this door and make it impossible to enter with a warrant. I have to tell you, I am stunned when I hear this, each time, because these are the exact same companies who are simultaneously mining customers' data for information and even selling it to third party companies. And they say it's okay.

The impact and magnitude of the Lawful Access crisis in the United States has grown to a point where the public safety trade-off to the citizens of this country can and should no longer be made privately and independently in the corporate boardrooms of tech companies. It must, instead, be returned to the halls of the people's democratically elected and publicly accountable representatives.

Ladies and gentlemen let me be very clear. The FBI supports the use of strong encryption. It's critical to securing our infrastructure and our online privacy. But there are already strong forms of encryption used daily in the US in the regulated financial and securities sectors, which secure information yet provide for appropriate access. We firmly believe that strong encryption models can be implemented by these companies in a way that is in accord with long-accepted Constitutional theories of privacy and civil liberties, continues to support robust cyber security, and provides for court-ordered lawful access.

Darrin Jones, FBI; President's Commission on Law Enforcement and the Administration of Justice; Crime Reduction Hearing, April 15, 2020.

I would reiterate the Technology Working Group's recommendation: **Federal legislation must be enacted to compel major technology companies to design for themselves strong encryption regimes for their products and services that protect privacy but that permit lawful access pursuant to the due process of law.**

Thank you for your time, and I look forward to your questions.