Statement for the Record by Mike Duffey

Assistant Special Agent in Charge

Florida Department of Law Enforcement

Before the Subcommittee on Consumer Protection and Commerce

Committee on Energy and Commerce

United States House of Representatives

"Holding Big Tech Accountable: Legislation to Protect Online Users"

March 1, 2022

Chairwoman Schakowsky, Ranking Member Bilirakis, and members of the Subcommittee, thank you for addressing this topic and for inviting me to provide my perspective. I serve as the Assistant Special Agent in Charge for the Florida Department of Law Enforcement, Cyber High-Tech Crime Unit. In my 25 years in law enforcement I have witnessed first-hand the revolutionary impact that technology has had on criminal investigations. I started my career during the AOL dial up days, and I'm sure some of you remember the sound your computer made when the modem made the connection.

Since then, law enforcement has had to learn how to properly investigate crimes committed using computers and mobile devices and the challenges that come with identifying evidence that is stored on devices, with the service providers, and in the cloud. In some ways the explosion of digital data means that we can obtain high-quality evidence that helps us solve crimes. In other ways, the rapid proliferation of platforms and data has created challenges that negatively affect our ability to detect and investigate criminal activity.

What I would like to convey to the subcommittee today is that when crimes are committed – both online and in the physical world – technology companies possess a large amount of the essential evidence law enforcement needs to do our job. But the lack of a regulatory framework that enables efficient access to that evidence means that we cannot be as effective at reducing online criminal threats or seeking justice for crime victims.

Social media has become the new "virtual playground" for today's youth, yet there are very few rules to govern that playground. Kids are able to follow viral "challenges" where they watch their peers consume laundry pods, climb milk crates, and perform blackout challenges to just name some. When you and I were their age, we certainly did some regrettable things, but it wasn't possible for thousands of people to watch what we did and try to imitate it within hours.

While age restrictions on most social media platforms prevent those younger than thirteen from joining, these rules are easily bypassed with the help of friends and parents. Thus, we see children of all ages

engaging online. While they can learn and play and socialize constructively on these platforms, they can also meet bad actors. We routinely see instances of "sexstortion" where underage children are threatened if they do not provide sexual images of themselves. The resulting self-production of images and video by these children yields content that can live online forever.

My investigative unit at FDLE, just like the thousands of other units like it across local, state, and federal law enforcement, is constantly improving our ability to obtain and analyze digital evidence. We need more resources to support that continuous improvement of our in-house capabilities, but we also need better cooperation – in a transparent and accountable way – from the technology platforms. We would like to see companies move from a reactive stance to a more proactive stance in which they are able to efficiently handle the large and growing volume of law enforcement legal process being served to them.

As the popularity of tech platforms continues to grow, and as new competitive options enter the market every day, those companies struggle to build out content moderation teams and maintain law enforcement outreach teams that are robust enough to handle our growing needs. To be clear, there are instances where some companies have shown a willingness to be more helpful with compliance because they understand their users are vulnerable to serious personal safety and security risks. But we have seen them hold back because they have no clear legal or regulatory framework that levels the playing field and enables them to protect their users' safety and bring bad actors to justice while avoiding liability or reputational risk.

It is past time for policymakers – together with stakeholders from industry, law enforcement, privacy communities – to generate the rules of the virtual playground and a system for enforcing them.

Most tech companies will insist that they are routinely providing law enforcement information when it is really needed in emergency – or exigent – circumstances. But determination of "exigency" is actually in the hands of the tech companies. We in law enforcement have the most relevant facts and context to determine exigency, yet the companies are the ones who have final say. This presents issues when law enforcement agencies receive complaints of individuals making online statements about causing harm to themselves or others. In one example, an individual made comments online regarding being "excited for July 9th and wanting to do what Nikolas Cruz did." Cruz was the murderer who took 17 innocent lives and injured 17 others at Marjory Stoneman Douglas High School in Parkland, Florida in 2018. This individual's social media postings indicated that they idolized Cruz and appeared to have visited the location where Cruz was arrested. Upon review of the information that law enforcement provided to the social media provider when asking for relevant information about the user, the company unilaterally made a determination that that they did not think the situation was an "imminent threat at this time".

In another example, we received a complaint of a younger male subject who was live-streaming himself discussing how he was going to commit suicide, potentially in front of a live audience. We immediately contacted the service provider after receiving the information in an attempt to determine where the user was located, while also noting that the live steam had appeared to have ended, but the live stream had ended. The content provider was unable to find a record of the streaming event. You can imagine the frustration of our investigators who were trying to prevent the unthinkable while dealing with a

provider who could not even verify that this was occurring on their platform. Thankfully in this particular instance, the subject's mother presented herself in front of the camera, on the individuals page and informed viewers that her son was safe and that she was handling the situation, with the assistance of local law enforcement.

Another ongoing challenge stemming from the lack of a standard framework governing the exchange of legal process between law enforcement and service providers is what we call the "word game" or "guess the magic word." Specifically, unless the terms we use in formal legal process documentation to obtain content from providers match their own unique corporate terms, law enforcement must engage in a lengthy back-and-forth that costs valuable time in an investigation – for example, in an online child sexual abuse investigation. A word that we think describes a specific type of data that we're looking for may be interpreted by the provider as something different, resulting in the provider telling us that they have no information that is responsive to our legal demand. The lack of uniform terminology therefore results in frustrating and dangerous delays in our investigations.

This challenge is compounded in some cases by the lack of a uniform timeframe for service provider response to law enforcement legal demands. Response time to legal process is up to the individual companies, which is in part limited by staffing at the provider, the volume of agencies requesting data, and the time it takes the provider to identify, extract, and return the specific the requesting agencies are seeking.

We are seeing some service providers implement online law enforcement portals that are designed to facilitate legal requests. These portals have been helpful in terms of improving timeliness and enhancing the security of data that is exchanged by both parties. In instances where there is not a portal companies typically establish an email address for law enforcement to email legal process. In rare instances companies have also identified a specific point of contact who can be reached should the need arise. Believe it or not, we still encounter companies that require legal demands to be faxed to them, and that send any responsive data back to us via fax.

The typical timeline for providers to respond to our legal requests is anywhere from one day to one month or longer. Regardless of whether a law enforcement agency or a judge sets a deadline for response in the legal documentation, the timeline for response is ultimately at discretion of the companies. Again, the lack of a standard legal process, language, or guidelines that govern law enforcement exchange with providers sometimes leads to dangerous delays in our investigations.

Service providers currently have no data retention requirements. In contrast, the banking industry is obligated to keep financial transaction records for a certain period of time. Money launderers and those conducting financial transactions for illegal economic activity certainly would prefer that information be deleted or removed at their discretion. Yet the tech platforms which – despite companies' efforts – are routinely used to facilitate a vast array of criminal activities are not subject to any retention requirements after a user chooses to delete content. There have been instances where law enforcement has tried to access content days or weeks after discovering that critical evidence might exist, only to find out that the content has been deleted by the provider.

Some of the most traumatic cases we deal with every day involve child sexual abuse material (CSAM). Service providers that identify illegal content such as CSAM on their platforms report this content to our vital partners at the National Center for Missing and Exploited Children (NCMEC), which is required by federal law. Providers retain that content until such time when law enforcement begins an investigation into these leads. Typically, the investigation begins with an agency serving legal process to a company for internet protocol information in an effort to identify a location where the activity was occurring. In most cases, this information is obtained with a subpoena because all the elements of probable cause have not been established. Further complicating these situations is that is illegal content is often posted to individuals' accounts without the provider or individual (hacked account) detecting it. In these instances, if law enforcement were to execute a search warrant at the residence of the account owner without knowing all the other relevant information such as login data, we could be executing a search warrant at the wrong location, due to someone else having posted the content after compromising the individuals account.

Each of these scenarios – which all levels of law enforcement encounter frequently – illustrate challenges that get in the way of our ability to protect the public and seek justice. The platforms that Big Tech has created have transformed society in many ways, some for the better, others less so. Users of these platforms should expect that the law enforcement officers charged with protecting them have a clear path to the evidence that they need to punish the guilty and exonerate the innocent. The establishment of a regulatory framework, including standardize legal process or guidelines that address these issues would benefit industry, law enforcement, and most importantly the citizens that we serve.

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