Questions for the Record from Senator Charles E. Grassley
U.S. Senate Committee on the Judiciary
"Protecting Innocence in a Digital World"
Submitted on July 16, 2019

Mr. Duffie Stone

1. Human traffickers know that children use social media and other internet platforms frequently, so they take advantage of apps, websites, and other platforms to exploit them. This is particularly concerning because of the constantly changing digital landscape.
    a. How can apps, websites, and other online platforms protect children from inappropriate content?

The intelligence analysts in my office confront this sort of exploitation regularly. They tell me better cooperation between law enforcement and social media platforms could help stem this problem – for agencies attempting to punish and prevent exploitation, and for the online companies serious about protecting the children on their platform from inappropriate content.

To illustrate what happens when this type of cooperation does not exist, consider a case in which someone in my office discovers evidence of criminal behavior on Facebook. The company provides no phone number to call for immediate attention, even if a fast response is critical to protecting a victim or stopping a predator. Instead, we must make a legal request through the Facebook law-enforcement portal, starting a process that typically takes three to six weeks to complete. It is also important to note that the Facebook security team purportedly has the ability to intercept nudity, pornography or violent videos the instant they are uploaded, yet the company doesn't communicate with local authorities when such content reveals potential criminal behavior. As a result, a post might come down quickly, but law enforcement cannot respond with similar alacrity – assuming they ever receive a report from Facebook at all. If either were the case, if law enforcement had a quicker pipeline to Facebook, or if the company had a way to report potentially criminal activity to local jurisdictions while the information is still actionable, we could significantly impact the way criminals use social media platforms to commit crime. If we had both, all the better.

Let me be clear: It is not my intent to single out Facebook. The company is not unique in its policies or in its operations. Most social-media platforms that I'm aware of are very difficult to deal with when it comes to helping law enforcement tackle criminal behavior. Let me also be clear that to some extent, this is understandable. These companies have legitimate concerns about maintaining users' privacy and participating in what might be misconstrued as state-mandated surveillance. Be that as it may, these platforms constitute one of many industries that must balance the privacy of their users with their duty to protect those same users from criminal predators. Child-care providers, educators, doctors, counselors and social workers must strike a similar balance. Surely, social-media providers can strike it as well. After all, they have an incentive to do so: providing safe haven for those who would sexually exploit children is not a business model that most Americans will accept.

Unfortunately, at present these companies seem more devoted to developing algorithms that prevent law enforcement from obtaining critical information. That leaves third-party vendors to come up with solutions to access the data. We see this, as well, with accessing encrypted cellular data for instance, on WhatsApp, which is a secure messaging platform. This type of app allows users to have the full access a standard phone would have, without being tracked. There are hundreds of other apps that are widely used that offer similar features. Those providing the hardware on which these apps operate also pose obstacles. Consider, for instance, Apple, with its iPhone security, which makes it difficult, if not impossible, for law enforcement to bypass, even when it has obtained a lawful court order for the information contained on the device. These examples outline the need for technology companies to come to the table with law enforcement and lawmakers to better protect children from bad actors and inappropriate content.

2. In 2018, the FBI seized Backpage.com, the most prominent online platform for sex trafficking and child exploitation.
    a. Has there been a migration of prostitution and sex trafficking activity from sites like Backpage.com to social media apps, since the FBI's seizure of Backpage.com? If so, how can we stop this activity?

Despite the great success of our federal partners, we have seen a migration of sex trafficking across other websites and social media platforms. My analysts tell me that when the Backpage site went down, numerous other sites emerged to fill the vacuum. CityXGuide.com and SkipTheGames.com now operate much as Backpage once did.

Dating apps like Plenty of Fish and Tinder are also widely used for prostitution. These apps allow you to use your location and set a radius within which you can find "willing" women. These accounts only show a few photos and offer a brief bio about that person. The photos are generally fakes used to lure in men. The app also features a messaging option that allows users to set up a date or talk about costs for whatever you intend to engage. Like Facebook, these apps are used for legitimate purposes, as well.

Facebook also has long hosted both fake and real accounts that further prostitution. In some instances, random pictures are pulled, and an account is made. It is not unusual to receive unsolicited friend requests from random accounts that purport to belong to women, posing semi-nude and offering links that allow you to contact them.

As for what can be done to stop the exploitation of such young women on these sites, I suggest watching closely the activity that takes place on them, rather than seeking to shut down the sites. That is particularly the case with sites that have other, legitimate applications. We know, for example, that if law enforcement wants to break up an organized crime ring and they find a place the mob or gang frequents, they surveil the location and gather enough evidence to make good arrests that allow for successful prosecutions. They don’t shut the place down. This is how we should approach these digital locations. Direct resources to state and local law enforcement so that they have the tech tools they need to conduct surveillance, gather evidence and shut down the underlying criminal activity. Bear in mind that, in many cases, the site is merely the conduit for criminal activity.