March 10, 2020

Dear Members of the Senate Committee on the Judiciary,

We are writing to oppose the "Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020". The bill is intended to address the sexual exploitation of children online, which is a serious and pressing issue. However, the measures proposed will create constitutional issues that reach far beyond their stated purpose. In particular, we are writing to address issues that would create or exacerbate existing problems in the criminal justice system.

The bill proposes a commission of 19 members who are tasked with making recommendations for best practices that would be presented to online providers. That commission is comprised of law enforcement, prosecutors, victims and victims' advocates, industry experts and technologists. It does include 2 members who have "current experience in matters related to constitutional law, consumer protection or privacy" but the provision is written so broadly that it does not guarantee any member will be experienced in the types of constitutional issues that would arise in the context of criminal prosecutions.

Concerning Delegation of Congressional Power to Create Criminal Law

Even if the Commission were more balanced, its role would still be concerning. The bill essentially gives the Commission and the Attorney General the power to make federal criminal law. This power should be reserved for Congress.

The bill provides that the Commission makes recommendations for best practices which then may be approved by the Attorney General. Although the bill requires Congress to approve those measures, it creates a streamlined process by which the bill must be introduced and voted on. This bars Congress from having time for meaningful consideration or debate and in-depth discussion will only happen in the context of the commission. Officers of interactive service providers must certify compliance with those best practices and face potential criminal penalties for false statements made in a certification. This empowers the Commission and the Attorney General, rather than Congress, to create the contours of what is considered criminal conduct.

This is an inappropriate delegation of criminal legislative authority away from Congress. Moreover, this bill would create a new crime and a new criminal penalty without containing any statutory notice or

explanation of what that crime will entail, which will only be knowable once the best practices are developed and issued. This raises serious due process concerns.

Potential for Fourth Amendment Violations

The bill also raises serious Fourth Amendment concerns. A recent letter from our colleagues at Tech Freedom dated March 5th, 2020 outlines certain Fourth Amendment issues in depth. We agree with that analysis. The proposed requirements do risk putting private companies in the position of becoming "government agents," creating the possibility that prosecutions will end in successful suppression motions arguing that the companies were required to obtain a warrant. This is a counterproductive outcome for achieving the legislation's intended goals.

Unfortunately, this measure reflects a disturbing trend in the age of ever-present digital data. Law enforcement now regularly seeks an end-run around warrant requirements contained in the Constitution by asking companies to search through people's private communications for evidence of alleged criminal activities. By essentially requiring businesses to actively search out unlawful material or information, they are urging companies to engage in a warrantless search where law enforcement would need a warrant to do the same if acting alone.

The bill also leaves open the very real possibility that the proposed best practices include encryption "back doors." Attorney General Barr has repeatedly made the case for a "golden key" to digital devices, stating "as we use encryption to improve cybersecurity, we must ensure that we retain society's ability to gain lawful access to data and communications when needed to respond to criminal activity."[1] Courts all the way up to the Supreme Court have held that digital devices are different and that the government should not be able to access such devices freely. Not only do encryption "back doors" make devices less secure for all that use them, but such a proposal would also require businesses to design products in order to make them accessible to law enforcement intrusion.

This is an extraordinary step that should not be considered acceptable under Fourth Amendment protections. When law enforcement obtains a search warrant they are allowed to search for the evidence they believe to be present whether in a home or on a digital device, but law enforcement should not be permitted to force companies to create products designed around law enforcement access. The warrant requirement was designed to be individualized given the abuses occurring under English common law. Even though the drafters of the Constitution would not have been able to envision many of the technologies we use today, these protections should still be upheld to avoid abuses of power by the government.

Contributing to Overcriminalization

The bill includes a criminal penalty carrying a two-year prison sentence for knowingly submitting a written certification of best practices that contains a false statement. This is concerning for a number of reasons. To begin with, this is the criminalization of a mere paperwork requirement. A person could be charged with a crime and face a prison sentence for a paperwork error regardless of whether any harm actually occurs. There is a significant likelihood that any best practices recommended by the Commission and ultimately promulgated by the Attorney General will be complex, may contain

[1] Katie Brenner, *Barr Revives Encryption Debate, Calling on Tech Firms to Allow for Law Enforcement*, NEW YORK TIMES, (July 24, 2019) https://www.nytimes.com/2019/07/23/us/politics/william-barr-encryption-security.html

specialized or technical terms, or will include undefined or vaguely defined concepts. This expands the possibility of a person facing a criminal prosecution based on a difference of interpretation of a vague definition of what the government's best practices require. It may also result in a two-tiered system where large companies can afford the necessary expertise to comply with these best practices and small businesses are left with a choice between incarceration and bankruptcy.

This provision is also redundant with existing law, which already broadly criminalizes making a false statement to the U.S. government.[2] Having multiple federal criminal laws that cover the same substantive conduct would allow prosecutors to pile on charges and additional years of incarceration. This contributes to the trial penalty--the disparity between the sentence a defendant receives when accepting a plea bargain and the much greater sentence he or she receives when exercising their right to trial. This trial penalty has virtually eliminated the constitutional right to a trial in the federal system.[3] It also contributes to the possibility of innocent people pleading guilty, because they fear the long and harsh sentence they would receive if wrongly convicted at trial. This bill would contribute to the trial penalty by creating a new crime and a new prison sentence for conduct that is already unlawful.

For the reasons listed above we urge you to oppose this legislation in its current form. If you have any questions you can contact Jumana Musa at jmusa@nacdl.org or Jeremiah Mosteller at jeremiah@idueprocess.org.

Sincerely,

Due Process Institute

National Association of Criminal Defense Lawyers

[2] 18 U.S.C. § 1001

[3] Rick Jones, et al., *The Trial Penalty: The Sixth Amendment Right to Trial on the Verge of Extinction and How to Save It*, National Association of Criminal Defense Lawyers, available at https://www.nacdl.org/trialpenaltyreport.