Opening Statement
Ranking Member Rob Portman
COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS
"SOCIAL MEDIA'S IMPACT ON HOMELAND SECURITY: PART I."
SEPTEMBER 14, 2022

AS PREPARED

Thank you, Chairman Peters, for holding this hearing. This past Sunday, we observed the 21st anniversary of the 9/11 terrorist attacks. Over the last two decades, the United States has adapted to combat the most pressing threats to our nation's security. The advent of social media has added a new dimension to the ever-evolving threat landscape and created new considerations for combatting terrorism, human trafficking, and other threats.

During last October's hearing on how algorithms promote harmful content, I examined how social media business models contribute to the amplification of terrorism and other dangerous activities. Since then, the Committee has identified ways in which social media companies' product development processes tend to conflict with user safety. Whistleblower testimony has revealed that in numerous occasions, the leaders at social media companies were aware that certain platform features increased threats to user safety and chose not to mitigate such concerns.

It is unfortunate that the American public must wait for whistleblower disclosures to find out about ways in which platforms are knowingly and unknowingly harming their users. The lack of transparency in the product development process, the obscurity of algorithms, and misleading content moderation statistics create an asymmetric information environment, in which the platforms know all, yet the users and policymakers know very little.

One consequence of this lack of transparency is related to the Chinese Communist Party. I have serious concerns about the opportunities that the Chinese Communist Party has to access TikTok's data on American users. There are over 100 million Americans, including 40 million under the age of 19, who use TikTok. This TikTok data remains vulnerable to the Chinese Communist Party both as the CCP tries to exploit its access to U.S. data and exert influence over the content that U.S. users see. For example, despite moving U.S. user data to servers in the United

States, TikTok and ByteDance employees in China retain the ability to access this data.

Also, we learned yesterday from Senator Grassley's opening statement in a Senate Judiciary Committee hearing with the Twitter whistleblower that Twitter failed to prevent Americans' data from being accessed by foreign governments. In fact, Senator Grassley spoke about how several Twitter employees were actually foreign agents of India, China, and Saudi Arabia, which is deeply concerning and speaks to why Congress needs more information from platforms on their securitization of user data.

Another consequence of poor transparency relates to content moderation. While I recognize that content moderation is a key component to creating safe platforms for users, it cannot be the silver bullet. Transparency reports released by companies often only detail the amount of content that has been removed for violating company policy. However, these reports do not account for violating content that is left up on the platform and goes undetected.

It also doesn't account for content that is incorrectly censored, as we often see with many conservative voices on social media. I, like many of my colleagues, have been critical of the political biases held by Big Tech platforms, which have resulted in systematic takedowns of accounts that hold ideologies with which the left and liberal media disagree. These takedowns are often done under the guise of combatting "misinformation" or "hate speech," when in fact they are really just combatting conservative viewpoints that conflict with their own. Any steps taken to address the impact of social media on homeland security must account for First Amendment protections and safeguard free speech.

For us to have a responsible conversation about the impact of harmful content on American users and homeland security, we need to talk about how current transparency efforts have been ineffective. Congress must enact legislation that will require tech platforms to share necessary data so that research may be done to evaluate the true extent of how harms from social media impact Americans.

That is why I have been working with Senators Coons and Klobuchar to create bipartisan legislation to do just that. The *Platform Accountability and Transparency Act* would require the largest tech platforms to share data with

vetted, independent researchers and other investigators so that we can all increase our understanding of the inner workings of social media companies and later regulate the industry based on what we learn.

I look forward to hearing from our witnesses and thank Chairman Peters for holding this hearing.

Opening Statement
Ranking Member Rob Portman
COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS
"SOCIAL MEDIA'S IMPACT ON HOMELAND SECURITY: PART II."
SEPTEMBER 14, 2022

AS PREPARED

Thank you, Chairman Peters, for holding this hearing to examine the impact of social media on homeland security. We had a productive hearing this morning on the topic, and I look forward to this hearing with industry representatives.

As of 2021, almost 72 percent of Americans used social media. And while social media has offered unprecedented connectivity, it has also raised serious concerns for our children, our civic culture, and our national security.

Terrorists, violent extremists, drug cartels, criminals, and other dangerous forces have used social media in furtherance of their violent goals. Perhaps the most concerning consequence of social media is the ability for our adversaries to exploit platforms to harm Americans for their own geopolitical gain. It is imperative for policymakers to identify and thwart China's exploitation of technology that furthers its espionage campaigns. In this second panel today, we will discuss China's influence over TikTok, a social media app that at least one-third of Americans use.

As the lead Republican on this Committee and previously as the Chairman of the Permanent Subcommittee on Investigations, I have been focused on China's malign activities. In 2019, I led a year-long bipartisan investigation which found that China recruits U.S.-based researchers to steal taxpayer-funded intellectual property and research for its military and economic gain through its Thousand

Talents Program. Following this report, I introduced my bipartisan legislation, the *Safeguarding American Innovation Act*, which seeks to stop U.S. taxpayer-funded research and intellectual property from falling into the hands of the Chinese Communist Party or CCP. Two months ago, I also issued a new report detailing China's efforts to target, influence, and undermine the U.S. Federal Reserve. China has a pattern of economic and cyber espionage, and social media is just another opportunity. I am highly concerned about TikTok and how China may be leveraging their influence to access the platform's data on Americans.

Chinese law requires all companies operating under its jurisdiction to, in essence, allow the Chinese Communist Party to access every piece of data collected. Any company that refuses to comply with the CCP's demands is subject to severe consequences. Therefore, since both TikTok, and its parent company ByteDance, are located in mainland China, we are left to assume that TikTok's user data could be accessed by the Chinese Communist Party.

That means that the CCP may have access to one hundred million Americans' personal and proprietary information. As our expert witness this morning testified, China's access to user data will allow it to extend its malign agenda and build dossiers on American citizens. The overwhelming popularity of the app with America's youth will allow China to collect never-before-accessed troves of data on our children—the future generations of American leaders.

But the challenges that social media poses to our children are not limited to TikTok. We continue to see the proliferation of child sexual abuse material online. I have been at the forefront of this fight for years. I am proud that my Stop Enabling Sex Traffickers Act was signed into law in 2018. This was the first bill to reform Section 230 by removing barriers to both criminal prosecution and civil suits against websites that knowingly facilitate online sex trafficking. Because of this change in law, courts are beginning to affirm that Section 230 cannot shield for internet companies when they fail to respond to images of child exploitation and continue to profit from exploitation on their platform. A specific case against Twitter is now being considered by the Ninth Circuit Court of Appeals and will show if the law needs to be expanded in order to protect children.

But it's not just Twitter, the fight continues on other platforms that are used to exploit children. Meta announced earlier this year that they would not report all

explicit images of children and would instead "err on the side of an adult" when moderating explicit images of could-be children. In other words, when the age of an individual in a sexual image is uncertain, content moderators are told to put their thumbs on the scales of that individual being an adult. This is outrageous. Let's be clear what we are talking about: child sexual abuse material are images of a minor's rape or exploitation. And somehow Meta has decided that these should not be referred to law enforcement? The National Center for Missing and Exploited Children has made it clear that images must be reported if they appear to involve a child so that law enforcement can intervene to stop the abuse and prosecute perpetrators.

I worked with colleagues across the aisle to craft SESTA narrowly so that it would be focused ending trafficking and exploitation online. But it may in fact be too narrow if companies continue to turn away from keeping this exploitation off of their platforms. I hope my colleagues will take up the challenge of revisiting SESTA and tightening the standard so that entities showing a reckless disregard for the exploitation of children are held accountable. I am ready to be an ally in this fight even after I leave the Senate.

I look forward to discussing these matters, especially regarding how product development processes appear to be at odds with user safety, as well as the need for more detailed transparency from the companies. Thank you, Chairman Peters, for holding this hearing.