REMARKS OF
COMMISSIONER GEOFFREY STARKS
BEFORE THE CONSUMER TECHNOLOGY ASSOCIATION'S
GOVERNMENT AFFAIRS COUNCIL

January 6, 2020

Thank you for that introduction and for the warm welcome to my first CES. I'm looking forward to spending the next few days seeing what's new about the cutting edge of technology and communications. CTA has asked me to spend a few minutes with you today talking about the most important issues on the horizon in technology and telecommunications and what I will be focusing on at the FCC. In 2020 and beyond, my principal focus will be ensuring that our communications networks and technologies support security, privacy, and our democratic values.

Here at CES, like everywhere else, we're all hearing a lot about 5G. Faster and more robust networks will enable new applications like driverless cars, virtual reality, and robotic surgery. Constant connectivity will create unprecedented amounts of data recording where we go, what we do, and who we're with—a "data big bang" that will significantly change how we interact with the world around us.

At the FCC, I've called for an increased focused on securing all of that data. We know our current networks and all who use them are vulnerable. That's why I have been working over the last year on a framework for removing untrustworthy equipment, particularly equipment from Huawei and ZTE, from our communications networks. Policymakers have good reason to be concerned. The Financial Times reported in 2017 that Chinese government-supplied Huawei servers at the African Union Headquarters in Ethiopia had been transferring sensitive information to servers in Shanghai every night, from midnight to 2 a.m., *for five years*.

Finding the untrustworthy equipment in our systems, fixing the problem by replacing it with more secure equipment (since no remedy short of that is sufficient), and funding such replacements is a big job that will take extensive coordination within and between government and industry. I remain committed to getting the job done, as thoroughly and quickly as possible. The rising tide of data created by new applications and technologies makes improving data security an urgent necessity, not a mere convenience.

I am optimistic that technological developments, especially 5G standards, will support our efforts to improve network and data security. 5G offers a variety of features—from virtualization to the expanded use of encryption—that will make these new networks more secure than 3G and 4G predecessors. But those features will only be effective if they are rigorously and consistently implemented. As I visit with experts here over the next few days, I will be asking about their plans to take advantage of these benefits, and about any other vulnerabilities we must be prepared to defend against.

Moving beyond security to the terrain of ethics, the rise of big data bestows a corresponding measure of 'big responsibility' upon all of us in the room. This is a critical moment. Like any such moment in the history of technology, it imports enormous optimism and opportunity, as well as the need for a healthy measure of clear-eyed analysis. Entities throughout society, from retailers to law enforcement, are in the process of deploying systems capable of analyzing enormous datasets in real-time in order to make complex, automated decisions about us. What could possibly go wrong? That common wisecrack should serve as our sober motto in this context. We must undertake, right now and continuously, the thorough examination of all these new capabilities to decide now how we will ensure that they are all poised to serve a future that creates opportunities instead of reinforcing existing inequalities. A lot could go wrong, and it will be on us to ensure that it doesn't happen on our watch.

Of course, the Age of Data has already begun. Entities already access our data—our browser history, the clothes we buy, the places we frequent. Programmed algorithms use this data to suggest songs, movies or even romantic partners. But, as next-generation networks become standard, an increasing number and variety of internet-connected devices will generate exponentially greater amounts of information about us. While uses of this data can be delightful, or at least harmless, they can also ultimately impact life-changing events like getting a mortgage or finding a dream job, or perhaps getting stopped by the police. These are moments that change individuals' lives for better or worse and, when taken together, shape our culture.

We're already seeing early warning signs that some of these uses may be creating a culture we won't want to live in. Reuters reported that Amazon discovered that its job applicant search algorithm excluded women because it flagged qualified applicants based on historical trends that favored men. It also penalized résumés that included the word "women's"—such as leadership of a women's club—and downgraded candidates from two women's colleges.

In 2018, the ACLU used facial recognition software to scan the face of every member of Congress against mugshots. That test generated 28 false positive matches, implying that these Representatives and Senators – including many from communities of color – were criminals. Local police departments already use similar software. Can you imagine the risk created by a false positive identification during a tense traffic stop? I can. We all must interrogate every version of this question in the context of the new data analysis capabilities that seem to appear every day.

This isn't the only example. The U.S. Department of Housing and Urban Development recently sued Facebook for violating the Fair Housing Act by allegedly mining users' data in a way that effectively blocked access to housing advertisements based on race, gender, religion and other protected characteristics.

The future will be even more complex. Insurance companies could use algorithms to deny life insurance to people who might otherwise qualify based on their actual health history. Government agencies could apply algorithms to benefit review applications. Algorithms may even determine the deployment of 5G wireless service, deciding who gets it and who doesn't. If the algorithm has embedded biases, people could be unfairly excluded.

With so much at stake, we cannot leave it to others to decide what our future will look like. More and more, we hear about China pushing ahead on technologies like artificial intelligence and facial recognition technologies. There is a perverse logic behind those advances: it's easier to develop widespread facial recognition, for example, in a country whose laws don't prioritize civil liberties or individual privacy. And China is exporting those systems to the world. Research by the Carnegie Endowment for International Peace suggests that at least 52 countries are testing facial recognition systems using Chinese technology.

There are, undoubtedly, legitimate and valuable uses for these technologies. But we need to be cautious—and mindful of concerns about accuracy, data protection, privacy, civil liberties, and the appropriateness of using of highly personal information. For the United States, that means taking a leading role in international discussions that will set norms and standards. Right now, we're not vocal enough in these discussions. Last month, the Financial Times reported that Chinese technology companies are shaping new facial recognition and surveillance standards being developed at the International Telecommunications Union—without input from human rights, consumer protections, or data security experts. If governments, organizations, and companies that value civil liberties don't get in the game, we may soon find ourselves living in a world that authoritarians shaped for us. We absolutely must not accede to that reality. Discussions like the ones you will have this week are an essential part of ensuring that those technologies develop in way that is consistent with our values.

We also cannot hand these culture-shaping decisions over to algorithms without significant human supervision. Algorithms aren't inherently good or bad, but they can create serious, far-reaching consequences. Machine learning and artificial intelligence are still developing, but we have enough experience now to know that these systems can, intentionally or not, replicate biases we cannot tolerate. Researchers at the National Institute of Standards and Technology found that most facial-recognition algorithms misidentify people of color more often than white men. In the study, Asian and African American people were up to 100 times more likely to be misidentified than white men. Native Americans had the highest false-positive rate of all ethnicities. Women more were more likely to be falsely identified than men.
Software is created by human beings, and it often reflects the conscious or unconscious bias of its creators or some persistent inequities in our society. Moreover, neither the software engineering workforce nor many datasets it analyzes reflect the diversity of the US population—the people who will be subject to these algorithmic decisions.

While some algorithmic bias may be corrected through greater transparency and scrutiny, the many Americans without access to technology or broadband may remain vulnerable. As artificial intelligence increasingly determines who sees opportunities for housing, education and employment, people on the wrong side of the digital divide may be rendered effectively invisible without the connected devices and internet speeds needed to be appropriately acknowledged by the data algorithms. Those in data deserts may never hear about the good job or the affordable mortgage, exacerbating growing inequality in this country.

In closing, though I have outlined a number of big challenges that I will be focusing on this year, I want to emphasize how optimistic I am about the next decade in our technological development. The Internet of Things, smart electrical grids, and autonomous vehicles all raise the stakes, but leaders like you are hard at work on those problems. If we work together, I am confident we can build a future that is more advanced, more secure and more prosperous, and more equitable for all. Thank you again for having me today.