

UNITED STATES OF AMERICA Federal Trade Commission WASHINGTON, D.C. 20580

Opening Remarks of Federal Trade Commissioner Rohit Chopra¹

You Don't Say: An FTC Workshop on Voice Cloning Technologies

Washington, D.C. January 28, 2020

Thank you all and welcome. According to recent surveys, Americans are losing trust in technology companies, and many are questioning their role and impact in society.

While we all know the benefits of new technologies and the immense fortunes showered on the companies creating them, many of us are concerned about how these technologies can be misused and abused.

Today, technology and data are weaponized by those who wish to do our country harm. We have seen how the harvesting of personal data can threaten our safety. Massive data breaches, from the Office of Personnel Management to Marriott and more, have been linked to actors in China. A Chinese gaming company was ordered by the Committee on Foreign Investment of the United States to divest its recent acquisition of Grindr, a popular gay dating app, as many suspected the data could be used for blackmail. Others use personal data to target and manipulate us with fake information to create social and political divisions, which can disrupt our democracy and economy.

Privacy is clearly now a national security issue. But it is not just about surveillance of our movements and our social interactions; new technology can now allow us to clone what we thought was uniquely ours: our biometrics. From our fingerprints to our faces, losing control of our own biometrics poses another level of peril.

When this happens, deepfakes, disinformation, and distrust will accelerate. We will need to determine how to control this technology and keep it out of the wrong hands.

To protect our safety and security from the dangers of biometrics theft, we will need to be forward-thinking, rather than waiting for massive harm to occur. This may involve new laws, licensing, export controls, and oversight.

Today, we will examine one element of biometrics: voice cloning.

-

¹ The views expressed below are my own and do not necessarily reflect those of the Commission or of any other Commissioner.

A goal of today's workshop is to learn more about this technology, its implications, and what can be done to confront the dangers it poses.

To that end, we will begin the day with a keynote presentation from Patrick Traynor, the John and Mary Lou Dasburg Preeminence Chair in Engineering at the University of Florida's Herbert Wertheim College of Engineering, who will discuss the state of voice cloning technology.

Following Professor Traynor's presentation, our first panel will discuss how voice cloning technology can be harnessed to enable people who have lost their voices due to injury or disease to speak again using realistic versions of their pre-injury and pre-disease voices, among other positive uses.

But we also will hear about the risks voice cloning technologies pose and how they are likely to be used in social engineering attacks.

The second panel will focus on how technologists, corporations, and society should evaluate these new technologies and whether they should impose controls on the technologies' introduction and availability.

The first two panels will tee up the last panel of today's workshop, which will examine whether technologies exist, or are likely to be created, that can mitigate the potential harms of voice cloning technology.

I look forward, as I'm sure you do, to a lively and informative discussion. With that, I'd like to thank the FTC staff who helped make this workshop a success, and all of you for your participation. And now I'll turn the microphone over to our keynote speaker, Professor Patrick Traynor.

Thank you.

###