Opening Statement
Chairman Frank Pallone, Jr.
Energy and Commerce Committee
Subcommittee on Consumer Protection and Commerce
Hearing on "Americans at Risk: Manipulation and Deception in the Digital Age"
January 8, 2020

Americans increasingly rely on the Internet for fundamental aspects of their daily lives. Consumers shop online for products ranging from groceries to refrigerators. They use the Internet to telecommute or to check the weather and traffic before leaving for the office. And they use social media networks to connect with family and friends and as a major source of news and information.

When consumers go online they understandably assume that the reviews of the products they buy are real, that the people on their social networks are human, and that the news and information they are reading is accurate. Unfortunately, that is not always the case.

Online actors, including nation-states, companies, and individual fraudsters, are using online tools to manipulate and deceive Americans. While some methods of deception are well known, many are new and sophisticated, fooling even the most savvy consumers. Today, technology has made it difficult, if not impossible, for typical consumers to recognize what's real from what's fake.

And why exactly are people putting so much effort into the development and misuse of this technology? Because they know that trust is the key to influencing and taking advantage of people. Whether for social, monetary, or political gain, if bad actors can make people believe a lie, they can manipulate us into taking actions we wouldn't otherwise take.

In some instances, we can no longer even trust our eyes. Videos can be slowed to make someone appear intoxicated. Faces can be photoshopped onto someone else's body. Audio can be edited in a way that takes a person's words out of context.

The extent of such manipulation has become extreme. Machine learning algorithms can now create completely fake videos, known as deepfakes, that look real. Deepfakes can show real people saying or doing things they never said or did.

For example, face-swapping technology has been used to place actor Nicholas Cage into movies he was never in. Actor-director Jordan Peele created a deepfake supposedly showing President Obama insulting President Trump. The most common use of deepfakes is non-consensual pornography, which has been used to make it appear as if celebrities have been videotaped in compromising positions. Deepfake technology was also used to humiliate a journalist from India who was reporting on an 8-year-old rape victim.

Advances in algorithms are also behind the glut of social media bots, automated systems that interact on social media as if they were real people. These bots are used by companies and other entities to build popularity of brands and respond to customer service requests. Even more alarming is the use of these bots by both state and non-state actors to spread disinformation, which can influence the very fabric of our societies and our politics.

And manipulation can be very subtle. Deceptive design, sometimes called "dark patterns," capitalize on knowledge of how our senses operate to trick us into making choices that benefit the business. Have you ever tried to unsubscribe from a mailing list and there's a button to stay subscribed that's bigger and more colorful than the unsubscribe button? That's deceptive design. Banner ads have been designed with black spots that look like dirt or a hair on the screen to trick you into tapping the ad on your smartphone. And there are many more examples.

Since these techniques are designed to go unnoticed, most consumers have no idea they are happening. In fact, they are almost impossible for experts in types of techniques to detect.

While computer scientists are working on technology that can help detect each of these deceptive techniques, we are in a technological arms race. As detection technology improves, so does the deceptive technology. Regulators and platforms trying to combat deception are left playing whack-a-mole.

Unrelenting advances in these technologies and their abuse raise significant questions for all of us. What is the prevalence of these deceptive techniques? How are these techniques actually affecting our actions and decisions? What steps are companies and regulators taking to mitigate consumer fraud and misinformation?

I look forward to beginning to answer these questions with our expert witness panel today so that we can start to provide more transparency and tools for consumers to fight misinformation and deceptive practices.