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

Office of Commissioner
Rohit Chopra

Prepared Remarks of
Federal Trade Commissioner
Rohit Chopra[1]

Common Sense Media
Truth About Tech Conference
April 4, 2019

Georgetown University
Washington, DC

Thank you for inviting me to join you today to talk about how we hold tech companies accountable for protecting privacy, especially for children.

As the debate on privacy and tech industry accountability heats up, it is worth reflecting on how we enforce or seek compliance with many of our laws. Policing markets is a daunting endeavor. The sheer number of businesses, the vast scale and scope of the biggest market players, and the complexity of business models and practices all serve to lower the probability of detecting illegal conduct. Ij EMC /mingrnie1 (m)-2 4 (l)]TJ 0 (l)-2 (e)4a dec f]TJ 04 (t)-2 (s)-nu for i dd 2 (va)4 (c) p ddfo

Today, I want to talk about the privatized privacy policing regimes created by the Children's Online Privacy Protection Act, or COPPA. These regimes raise questions about the efficacy of relying on private parties paid by regulated entities, given that these "regulators" may lack the right incentives to crack down on the very companies that pay their bills. As we consider different approaches to privacy law enforcement and tech industry oversight, we should be wary of these distorted incentives.

Privatized Privacy Police

According to a survey conducted by the FTC in 1998, 89 percent of commercial websites geared to children collected personal information, but only one percent required parental consent for the collection or disclosure of that information.[2] Later that year, just over twenty years ago, Congress passed COPPA.

While COPPA authorizes state attorneys general to enforce the law, it does not give parents the right to have their day in court with companies that illegally spy on their kids. Instead, it creates a privatized policing mechanism to supplement government enforcement, known as the Safe Harbor program. This program allows approved Safe Harbor organizations to oversee program participants' websites and apps for compliance. In exchange for enrolling and maintaining good standing, companies are shielded from formal enforcement actions by the FTC.

Just a quick summary of how these Safe Harbor provisions work. Industry groups and other organizations can seek a vote from the FTC to administer a Safe H

well as other law enforcement agencies across the country, identify trends and take action when complaints start piling up. While one interpretation of this finding is that everything is hunky dory and there's nothing to look at here, I'm not so sure. For example, in our analysis, we sometimes had trouble finding how to file a complaint. We also think many parents would find the forms confusing or cumbersome to complete. It's natural to wonder whether these organizations have the right incentives to seek out complaints.

Second, few Safe Harbor programs discipline or suspend operators for noncompliance with their rules. When online operators violate the rules, Safe Harbor programs typically try to bring websites or apps into compliance, rather than bring formal disciplinary action. However, we should always be asking whether privatized policing mechanisms primarily see entities as clients, rather than companies they must watch over.

It is worth noting that one entity operating a Safe Harbor program has run into trouble. In 2014, the FTC took action against the TRUSTe certification program,[7] which also assists online operators with complying with cross-border privacy frameworks, such as the EU-US Privacy Shield and APEC guidelines. TRUSTe, which is operated by a for-profit company known today as TrustArc, failed to conduct promised annual recertifications of companies participating in its privacy seal program more than 1,000 times between 2006 and 2013. In 2017, the New York Attorney General also took action against TRUSTe for failing to conduct adequate assessments under the COPPA Safe Harbor program.[8]

After the FTC action was announced, our host today, James Steyer, submitted a comment letter into the TRUSTe docket, asking the Commission to revoke TRUSTe's approval as a COPPA Safe Harbor program. While this predated my time as a Commissioner and I don't know the details of any deliberations, the Commission replied to Common Sense Media that "[t]he Commission regards the ability to revoke an organization's safe harbor status as an important mechanism to ensure the integrity of the program."[9] I agree.

Privacy Path Forward

So what are the implications for COPPA and the broader debate on privacy, security, and accountability for the tech sector? How should we assess industry arguments for self-regulatory provisions in any forthcoming federal privacy legislation?

We need to be clear-eyed about the distorted incentives of privatized privacy policing. Whether it is programs like Safe Harbor or the reliance on third-party private-sector assessors, it is hard for anyone to bite the hand that feeds them. Whenever regulated entities pay fees and shop for a regulator, are there the right incentives

settings, like when banks moved from bank charters to regulators eager for their fees or when for-profit universities shopped around for their accreditors. The results can be devastating.

To mitigate the concerns about distorted incentives and regulatory capture, the FTC should make more documents about the Safe Harbors public. In