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. It only becomes more improbable when you add rapidly evolving technology to the equation.

A single government agency rarely has the resources that these industries can marshal to their defense. That's why laws often provide multiple avenues for holding companies accountable. For example, laws can grant citizens and other private parties with the ability to enforce the law. Congress typically respects the role of state law, another critical component of any effective enforcement regime. Given the power and influence of many industries over individuals, this all-hands-on-deck approach is essential.

Sometimes enforcement is outsourced to privatized policing mechanisms under the auspices of adding to or freeing up government resources. This can take the form of requiring the market to pay private companies to conduct independent reviews, assessments, and audits. Other times, laws provide for so-called self-regulatory solutions – like the one currently in focus with the Federal Aviation Administration's approach to overseeing Boeing or the accreditation system that oversaw the rise of predatory for-profit colleges. Some of these self-regulatory approaches shield companies that pay fees to a private company that will examine them.

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

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 Harbor program. Once approved, they can start enrolling and charging fees to "operators," the companies that run websites and apps.

Rules under COPPA spell out the requirements by which the FTC should evaluate any application to become an approved Safe Harbor program.[3] Programs must lay out the guidelines that operators must follow in order to participate. Programs must also ensure that they will independently assess operators for compliance with their program's guidelines, including by conducting a review of the operators' policies and practices at least one time per year. In addition – and this one is important – the programs must have robust disciplinary mechanisms for operators.

Our rules spell out examples of potential disciplinary actions, including: mandatory public reporting of any action taken against the operator; redress to consumers; voluntary fines paid to the Treasury; and referrals of violators to the FTC.

What do companies get in return for enrolling with a Safe Harbor? As the name suggests, they are deemed to be in compliance with the law's substantive requirements on parental consent, parental right of access to data, parental right of data deletion, security of data, and limitations on third-party sharing, among others. A recent FTC announcement plainly stated, "[c]ompanies that

[2] Press release, FTC, New Rule to Protect Children's Online Privacy Takes Effect April 21, 2000 (Apr. 20, 2000), https://www.ftc.gov/news-events/press-releases/2000/04/new-rule-protect-childrens-online-privacy-takes-effect-april-21.
[3] 16 C.F.R. § 312.11.

comply with an FTC-approved safe harbor program are exempt from agency enforcement action under the Rule."[4]

To be clear, this means that the Federal Trade Commission is blessing a private organization with developing rules, monitoring for compliance, and disciplining those that break those rules. In exchange, these private organizations earn fees, and companies get extremely favorable treatment under the law.

Now, like any enforcer, I like to see good faith efforts to comply with the law. For example, when companies retain third parties to kick the tires on their privacy practices, that's one piece of evidence that might suggest they are trying to comply. In many arenas, this factor carries weight when exercising prosecutorial discretion.

But should companies be able to pay a private party to give them free pass? While these COPPA Safe Harbor programs are certainly helping companies see how they can improve their practices, these self-regulatory organizations may have conflicting incentives, especially those that operate as for-profit entities. As we look to a future framework in any new privacy law, I fear that these privatized policing mechanisms could lead to online services paying private organizations primarily to avoid legal consequences when they violate the law.

Watching the Watchdogs

Since the finalization of the initial COPPA rules, the FTC has voted to approve several programs, including Aristotle International, Children's Advertising Review Unit, Entertainment Software Rating Board, iKeepSafe, kidSAFE, PRIVO, and TRUSTe.[5] These Safe Harbors in turn oversee hundreds of firms that operate scores of websites and apps directed to kids.

Erie Meyer, my office's Technologist, and I worked with FTC staff to obtain and analyze documents and data about the Safe Harbor programs. We specifically examined a recent year of annual reports that Safe Harbors are required to file with the FTC. I want to share two of our findings with you today.

First, the programs generally received very few, often zero, complaints, even though many Safe Harbor programs have specific guidelines to give parents the ability to file complaints directly with them.[6]

Consumer complaints are a critical vehicle for effective enforcement. The FTC's Consumer Sentinel tool – a repository for consumers to file law enforcement tips – has helped the FTC, as

[4] Press Release, FTC, FTC Approves Modifications to Video Game Industry Self-Regulatory COPPA Safe Harbor Program (Aug. 14, 2018), https://www.ftc.gov/news-events/press-releases/2018/08/ftc-approves-modifications-video-game-industry-self-regulatory.
[5] FTC, COPPA Safe Harbor Program, https://www.ftc.gov/safe-harbor-program.
[6] *See* PRIVO's Membership Agreement at 16 Sec. 9d (June 27, 2013), https://www.ftc.gov/system/files/attachments/press-releases/revised-childrens-online-privacy-protection-rule-goes-effect-today/130701privosafeharbor.pdf; *See also* CARU's Policies and Procedures at 3 Sec. 2.2, https://www.ftc.gov/system/files/attachments/press-releases/revised-childrens-online-privacy-protection-rule-goes-effect-today/130701carusafeharborapp.pdf.

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 for the regulators to be tough? Or might the incentives lead to competition on who can be the most lax and forgiving? We have seen this in other

[7] Press Release, FTC, FTC Approves Final Order In TRUSTe Privacy Case (Mar. 18, 2015), https://www.ftc.gov/news-events/press-releases/2015/03/ftc-approves-final-order-truste-privacy-case.
[8] Press Release, N.Y. Att'y Gen., A.G. Schneiderman Announces $100,000 Settlement With TRUSTe Over Flawed Privacy Certification Program For Popular Children's Websites (Apr. 6, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-100000-settlement-truste-over-flawed-privacy-certification.
[9] Letter to James P. Steyer of Common Sense Media, In the Matter of TRUSTe, Inc., File No. 1323219 (Mar. 12, 2015), https://www.ftc.gov/system/files/documents/cases/150318trust-eletters.pdf.

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 my recent voting statement in the Uber data security law enforcement action, I also argued for greater disclosure of third-party assessor and audit reports that the FTC has required in so many of its privacy and security settlements, including its orders with Facebook, Google, Twitter, and many others.[10] By subjecting these reports to more sunshine, it can counteract some of the incentives that might lead to lax oversight.

In addition, we must make it clear that we are willing to revoke an organization's Safe Harbor status or dismiss a third-party assessor hired as part of a remedial order against a company violating the law. If they are not properly policing privacy, they need to go.

The bottom line is that we must be more skeptical about outsourcing privacy oversight. Absent hard data that shows this privatized policing is actually effective, Congress should stick to mechanisms that work: real penalties that deter and are enforced by many, not just a few. I don't just mean financial penalties. Congress should also make sure we pursue the individuals who called the shots or who purposely turned a blind eye to privacy intrusions and failures. In some cases, we also need to shut down business models that are fundamentally broken.

If we want a marketplace that truly works, we need to spur meaningful competition, curtail conflicts of interest, and create real consequences for those violate the law. Everyone, especially parents and law-abiding online services, should welcome tough enforcement.

Thank you.

###

[10] Statement of Comm. Chopra In the Matter of Uber Technologies Inc. Commission File No. 1523054 (Oct. 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1418195/152_3054_c-4662_uber_technologies_chopra_statement.pdf.