Responses to Written Questions Submitted by Honorable John Thune to Rohit Chopra

Question 1. Vertical mergers such as the merger between AT&T and Time Warner have garnered some attention lately. The Federal Trade Commission (FTC) and the Department of Justice (DOJ) have not updated vertical merger guidance since 1984. Do you believe that the FTC and DOJ should issue new guidance on vertical mergers?

Response. Vertical mergers can threaten competition. For example, as I noted in my dissenting statement in the *Fresenius/NxStage* matter, vertical mergers can make it tougher for a new business to get off the ground.
Senior officials in the antitrust agencies have openly communicated that the 1984 guidelines do not provide useful guidance.[1]
It is troubling that the agencies have published guidance that we do not actually follow. I am very open to the idea of updating these guidelines.

Question 2. Government lawsuits to stop mergers are litigated using different procedures depending on which agency, the FTC or DOJ, handles the case. Do you think Congress should take action to ensure that agencies follow the same procedures, or do you support another approach?

Response. While I appreciate the theoretical concerns that have been raised, it does not appear that this has much real world impact. There are broader issues that stem from the FTC and DOJ having concurrent jurisdiction in merger review that Congress might consider giving a higher priority for examination. For example, thought should be given to ways to improve our clearance process.

Question 3. Should Congress amend Section 5(n) of the FTC Act, which addresses unfair practices, to clarify what constitutes "substantial injury?" If so, how?
Response. Both the courts and the Commission have identified various types of injury that meet this criterion. If there are additional types of injury that Congress wishes to codify, I am happy to work with you to determine how to best achieve those goals.

Question 4. Should the FTC issue more guidance to marketers on the level of support needed to substantiate their claims? If so, when do you anticipate that such guidance could be issued?

Response. Both consumers and marketers that are interested in complying with the law benefit from FTC guidance. Given case law, the Commission's Policy Statement on Advertising Substantiation, and other Commission statements, there is certainly an array of information to assist marketers with compliance, but I am always open to hearing ways to improve information to help law-abiding businesses.

Question 5. In June, the 11th Circuit vacated the Commission's data security order against Lab-MD. What effect, if any, will this have on the Commission's data security orders going forward?

---

[1] *See* D. Bruce Hoffman, Vertical Merger Enforcement at the FTC, Prepared Remarks for Delivery at the Credit Suisse 2018 Washington Perspectives Conference (Jan. 10, 2018), *available at* http://www.ftc.gov/system/files/documents/public_statements/1304213/hoffman_vertical_merger_speech_final.pdf.

Response. Given this decision, as well as feedback from stakeholders and our recent hearing on data security, we are actively engaged in discussions on how our orders can provide optimal deterrence under our existing Section 5 authority.

Question 6. If federal privacy legislation is passed, what enforcement tools would you like to be included for the FTC?

Response. Federal privacy legislation needs enforcement teeth to be effective. In addition to strong civil penalty authority, it would be useful for the FTC to have independent litigating authority. Commission fines must be strong enough to realign market incentives, rather than representing a cost of doing business. I look forward to working with Congress to identify additional tools and authorities to make any legislation effective.

Question 7. During the hearing, I asked the Chairman whether the FTC would consider using its section 6(b) authority to study consumer information data flows, specifically sending requests to Google, Facebook, Amazon, and others in the tech industry to learn what information they collect from consumers and how that information is used, shared, and sold. I believe the FTC's section 6(b) authority could provide some much needed transparency to consumers about the data practices of large technology companies, and help identify areas that may require additional attention from lawmakers. What are your views with respect to the FTC potentially conducting a study pursuant to section 6(b) of the Federal Trade Commission Act on the data collection, use, filtering, sharing, and sale practices of large technology companies such as Google, Facebook, Amazon, and others?

Response. Yes, the FTC should pursue a 6(b) study about the practices in the technology sector. This will help advance our competition and consumer protection mission. The FTC's research function is fundamental to how we should work to make markets fair and effective.

Responses to Written Questions Submitted by Honorable Jerry Moran to Rohit Chopra

Question 1. Section 5(a) of the *FTC Act*, which prohibits "unfair or deceptive acts or practices in or affecting commerce" is the legal basis for a body of consumer protection law that covers data privacy and security practices. The FTC has brought hundreds of cases to date to protect the privacy and security of consumer information held by companies of all sizes under this authority. The FTC staff recently submitted comments to the National Telecommunications and Information Administration (NTIA) that clearly indicate the FTC staff's view that the FTC would be the appropriate agency to enforce a new comprehensive privacy legislative framework. Do you agree with the staff's view?

Response. It is clear that data is playing an ever-increasing role in shaping all markets. From banking to real estate to travel to health care, every industry is relying on more and more data. Federal legislation should avoid problems of regulatory arbitrage that can impede federal enforcement. Even if the FTC has enforcement authority over a new law, it will be critical to ensure that this supplements, and does not supplant, the role of state law enforcement.

Question 2. As Congress evaluates opportunities to create meaningful federal legislation to appropriately ensure privacy of consumers' data, there have been suggestions to increase the FTC's authorities to enforce in this space. Will you commit to working with this Committee in measuring what resources, if any, will be needed to allow the agency to enforce any additional authorities that may or may not be provided in federal legislation?

Response. Yes.

Question 3. Sharing responsibilities with the DOJ's Antitrust Division, the FTC enforces antitrust law in a variety of sectors as described by your testimony. While the vast majority of premerger filings submitted to enforcement agencies do not raise competition concerns, the FTC challenged 45 mergers since the beginning of 2017, and of those, the FTC only voted to initiate litigation to block five transactions. Would you please describe the resource needs of the agency associated with hiring qualified outside experts to support its litigation efforts? Please explain how developments in the high-technology sector are accounted for in the FTC's decision-making process related to antitrust enforcement.

Response. Expert spending is costly. Compared to other statutes we enforce, our antitrust laws lack clear presumptions and rules, making litigation lengthy and resource-intensive. Given the state of the law, it is necessary to ensure adequate resources for litigation.
To be seen as an effective and credible enforcer, we must have enough qualified experts to collect and analyze data on business practices in the technology sector.

Question 4. Earlier this year, I introduced legislation called the *Senior Scams Prevention Act* with Senator Bob Casey to combat continued and increasingly complex attempts to defraud one of the nation's most vulnerable populations, our senior community. This bill seeks to ensure retailers, financial institutions and wire transfer companies have the resources to train employees to help stop financial frauds and scams on seniors. Would you agree that awareness and

education, guided by "best practices" established by industry and government partners, is a valuable tool in preventing consumer harms against our nation's seniors?

Response. Older Americans are disproportionately affected by fraud, and any effort to enlist industry and government in protecting them from the worst abuses is commendable. Educational initiatives can complement aggressive enforcement of those who defraud older American consumers.

Question 5. In its comments submitted to NTIA on "Developing the Administration's Approach to Consumer Privacy," the FTC discussed the various cases that it has taken up to address privacy-related harms to consumers, and it specifically noted four categories of harms: financial injury, physical injury, reputational injury, and unwanted intrusion. Could you please briefly describe each category while noting any FTC enforcement considerations specific to that type of harm?

Response. The FTC staff comment identified financial injury, physical harm, reputational injury, and unwanted intrusion as four categories of privacy harms that FTC enforcement actions have acted to address. *Financial injury* is the injury that an act or practice causes to a consumer's financial position. The NTIA comment notes that financial injury manifests in a variety of ways, including through fraudulent charges, delayed benefits, expended time, opportunity costs, fraud, and identity theft. Consumers may also suffer financial injury when they purchase a product sold through deceptive representations. *Physical injuries* include risks to individuals' health or safety, including the risk of stalking or harassment. *Reputational injury* involves disclosure of damaging private facts about an individual. And *unwanted intrusion* includes both activities that intrude on the sanctity of people's homes or intimate lives and commercial intrusions.
Through its enforcement of particular statutes or rules, like the Fair Debt Collections Practices Act, Telemarketing Sales Rule, and COPPA, the FTC vindicates particular legislative and regulatory judgments meant to prevent harms such as these.
This effort to categorize privacy harms should not be seen as creating an exclusive list or harms, nor should it be read to exclude from FTC scrutiny activities that may not directly implicate these types of harm. For example, the FTC Act prohibits companies from making certain misrepresentations in connection with privacy and data security. To the extent that a company acts in a manner that is deceptive under the law, the FTC must be able to take appropriate action.

Question 6. In the FTC's recent comments in NTIA's privacy proceeding, the FTC said that its "guiding principles" are based on "balancing risk of harm with the benefits of innovation and competition." Would you describe what this means, how you strike this balance, and how it is applied in practice under your Section 5 authority in the *FTC Act*?

Response. The FTC's staff comment reflects the fact that many of the FTC's enforcement efforts related to privacy and data security have proceeded under the FTC's Section 5 unfairness authority. Section 5(n) of the FTC Act requires that the FTC weigh the actual or likely substantial injury of an act or practice against countervailing benefits to consumers or competition. The FTC must be sure that it is not over- or under-estimating either side of the balance. Of course, Section 5's deception standard does not require this balancing exercise.

Question 7. The FTC's comments pertaining to "control" in NTIA's privacy proceeding stated, "Choice also may be unnecessary when companies collect and disclose de-identified data, which can power data analytics and research, while minimizing privacy concerns." How would the FTC suggest federal regulation account for de-identified data, if at all?

Response. While companies may sometimes claim that data has been "de-identified," in some cases these data can be easily "re-identified." We would be happy to work with you should you choose to specifically legislate on this issue.

Question 8. Your testimony indicated that continued technological developments allow illegal robocallers to conceal their identities in "spoofing" caller IDs while exponentially increasing robocall volumes through automated dialing systems. These evolving technological changes mean that the critical law enforcement efforts of the FTC cannot be the only solution, and your testimony described the additional steps the FTC is taking to develop innovative solutions to these issues. Would you please describe the process and outcomes of the four public challenges that the FTC held from 2013 to 2015? Are there plans to incentivize innovators to combat robocalls in the future?

Response. The FTC's process for its robocall challenges included public announcements, committees with independent judges, and, in some cases, cash prizes awarded under the America COMPETES Reauthorization Act.[2] To maximize publicity, the FTC announced each of its four challenges in connection with public events. The FTC announced the first robocall challenge at the FTC's 2012 Robocall Summit. In 2014, the FTC conducted its second challenge, "Zapping Rachel" at DEF CON 22. The FTC conducted its third challenge, "DetectaRobo," in June 2015 in conjunction with the National Day of Civic Hacking. The final phase of the FTC's fourth public robocall challenge took place at DEF CON 23. When the FTC held its first public challenge, there were few, if any, call blocking or call labeling solutions available for consumers. Today, two FTC challenge winners, NomoRobo and Robokilller, offer call blocking applications, and there are hundreds of mobile apps offering call blocking and call labeling solutions for cell phones. Many home telephone service providers also now offer call blocking and call labeling solutions. The FTC will not hesitate to initiate additional innovation contests if it identifies further challenges that could meaningfully benefit consumers by reducing the harm caused by illegal robocalls.

In addition to developing call blocking and call labeling technology, the telecom industry has also developed call verification technology, called STIR/SHAKEN, to help consumers know whether a call is using a spoofed Caller ID number and assist call analytics companies in implementing call blocking and call labeling products. If widely implemented and made available to consumers, the STIR/SHAKEN protocol should minimize unwanted calls. Certain industry members have begun to roll out this technology and it is in beta testing mode. We will keep a close eye on this industry initiative and continue to encourage its implementation.

[2] *See* "Details About the FTC's Robocall Initiatives" at https://www.consumer.ftc.gov/features/feature-0025-robocalls

Question 9. Would you please describe the FTC's coordination efforts with state, federal, and international partners to combat illegal robocalls?

Response. The FTC frequently coordinates its efforts with its state, federal, and international partners. The FTC often brings robocall enforcement actions with states as co-plaintiffs. For example, in the FTC's case against Dish Network, litigated for the FTC by the Department of Justice, the FTC brought the case jointly with California, Illinois, North Carolina, and Ohio. Collectively, the states and the FTC obtained a historic $280 million trial verdict.[3]

The FTC also coordinates outreach and education with the FCC. In 2018, the agencies co-hosted two robocall events— a policy forum that discussed technological and law enforcement solutions to the robocall problem[4] and a public expo that allowed companies offering call blocking and call labeling services to showcase their products for the public.[5] Additionally, the FTC and FCC hold quarterly calls, speak regularly on an informal basis, and coordinate on a monthly basis with our state partners through the National Association of Attorneys General. The FTC also engages with international partners through participation in international law enforcement groups such as the International Consumer Protection Enforcement Network, International Mass Marketing Fraud Working Group, and the Unsolicited Communications Network (formerly known as the London Action Plan).

Question 10. Your testimony described the limitations of the FTC's current data security enforcement authority provided by Section 5 of the *FTC Act* including: lacking civil penalty authority, lacking authority over non-profits and common carrier activity, and missing broad APA rulemaking authority. Please describe each of these limitations and how adjusted FTC authority to address these items would improve the protection of consumers from data security risks.

Response. As a general matter, the FTC Act does not provide the Commission with the authority to seek civil penalties from first-time violators of Section 5. Providing the FTC with expanded civil penalty authority would assist the FTC in its efforts to deter illegal conduct. Without civil penalties, companies with unlawful privacy and security practices get a free bite at the apple. Strong civil penalties and clear rules of the road are critical to deter lax privacy and security practices.

The FTC Act excludes or exempts non-profits and common carriers from the FTC's jurisdiction, but non-profits and common carriers rely on consumer data just as other persons subject to the FTC's jurisdiction do. Broadened FTC authority that also covers non-profits and common

---

[3] Press Release, FTC and DOJ Case Results in Historic Decision Awarding $280 Million in Civil Penalties Against Dish Network and Strong Injunctive Relief for Do Not Call Violations (June 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/06/ftc-doj-case-results-historic-decision-awarding-280-million-civil. The case is on appeal before the Seventh Circuit Court of Appeals.

[4] Press Release, FTC and FCC to Host Joint Policy Forum and Consumer Expo to Fight the Scourge of Illegal Robocalls (Mar. 22, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-host-joint-policy-forum-illegal-robocalls.

[5] Press Release, FTC and FCC to Co-Host Expo on April 23 Featuring Technologies to Block Illegal Robocalls (Apr. 19, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/ftc-fcc-co-host-expo-april-23-featuring-technologies-block-0.

carriers will eliminate opportunities for arbitrage and help ensure that persons collecting, storing, using, disposing of, or transporting consumer data do so in accordance with consistent rules.
The FTC Act provides the FTC with authority to issue rules that define with specificity acts or practices in or affecting commerce that are unfair or deceptive. Through this authority, the FTC could issue rules pertaining to data privacy and security. Unfortunately, this rulemaking must be conducted in accordance with the Magnuson-Moss Warranty Act, which adds time-consuming requirements to the rulemaking process that go well-beyond the requirements of the Administrative Procedure Act. Granting the FTC the authority to issue data security rules in accordance with the Administrative Procedure Act would allow the Commission to issue timely and appropriate rules that keep pace with technological development and seek civil penalties if companies violate them.