Responses to Written Questions Submitted by Honorable John Thune to Rebecca Slaughter

Question 1. Vertical mergers such as the merger between AT&T and Time Warner have garnered some attention lately. The FTC and 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. Given the enormous impact that vertical mergers could have on the economy, markets, and consumers, I think the Commission should closely scrutinize them, particularly when they involve oligopoly markets and markets with high barriers to entry.[1] There is broad agreement that the 1984 non-horizontal guidelines do not reflect the Commission's current enforcement practice. Indeed, Commission investigations and cases have identified a range of competition concerns arising from vertical mergers, including limiting access to or raising the costs of key inputs, restricting access to an important customer, inhibiting entry by new competitors, evading regulations, facilitating coordination, and anticompetitive information sharing. I recently urged the Commission to routinely conduct retrospective examinations of vertical merger enforcement decisions. This would allow the Commission to see if its predictions about a merger were correct and facilitate the Commission's ability to take any necessary enforcement action. The Commission is considering whether the agencies should issue guidance on vertical merger enforcement and such retrospectives would be critical to informing such an endeavor.

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. I do not think Congress should take action to change the procedures used by the Federal Trade Commission to carry out its merger enforcement mission. Congress intentionally created the Commission as an antitrust enforcement entity distinct from the DOJ. Accordingly, the FTC Act provides the Commission with additional tools to study markets and enforce the laws that are critical to our mission. Specifically, the administrative litigation process has been enormously useful in developing certain aspects of the law regarding mergers, such as mergers between hospitals. I do not share the concern some have articulated that the different statutory procedures between the agencies produce different outcomes; to the contrary, I think it is widely recognized that, in order to block a transaction, the DOJ and Commission both must show that a transaction would likely be anticompetitive.

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?

---

[1] For my detailed views on vertical mergers, please see my statement dissenting from *In the Matter of Sycamore Partners, Staples, and Essendant*, No. 181-0180 (Jan. 28, 2019), https://www.ftc.gov/system/files/documents/public_statements/1448321/181_0180_staples_essendant_slaughter_statement.pdf.

Response. The Commission has alleged and Courts have found that "substantial injury" can take the form of financial, physical, or reputational injuries. In addition, the Commission has alleged and Courts have found that "substantial injury" can take the form of an unwanted intrusion into the sanctity of people's homes and their intimate lives. As a general matter, there is no need to clarify what constitutes "substantial injury" under Section 5(n) of the FTC Act.
In many areas, however, the FTC also has specific rules that allow it to target specific law violations and seek monetary penalties without having to demonstrate or quantify "substantial injury." For example, while abusive telephone calls are an unfair practice that cause substantial injury in the form of an unwanted intrusion into consumers' homes that wastes their time, the Telemarketing Sales Rule sets out with specificity which practices are abusive and imposes a penalty for violations. This gives clarity to business and reduces the Commission's enforcement burden of having to prove that the calls amounted to "substantial injury" in each case. I believe the Commission would benefit from the authority to issue similar rules in the areas of privacy and data security, both to give clarity to business and to reduce the Commission's enforcement burden of having to prove that each data breach causes "substantial injury" to consumers.

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. The FTC has issued extensive guidance over the years to help marketers in determining the level of support needed to substantiate claims. The Commission first articulated the relevant factors used to determine the level of evidence required to substantiate objective performance claims in *Pfizer, Inc.*, 81 F.T.C. 23 (1972). Those factors included the type of claim, type of product, the consequences of a false claim, the benefits of a truthful claim, the cost of developing substantiation for the claim, and the amount of substantiation experts in the field believe is reasonable. The Commission and the courts have reaffirmed this standard many times since 1972.[2] In addition, the FTC also has provided extensive guidance through Guides and staff guidance documents.[3] Finally, FTC staff provide additional guidance through speeches and presentations to industry trade groups and industry attorneys.

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?

Response. The Eleventh Circuit determined that the mandated data security provision of the Commission's LabMD Order was insufficiently specific. The opinion did not have any effect on the FTC's use of Section 5 to protect consumers from deceptive or unfair data security practices. The Commission is engaged in an ongoing process to craft appropriate order language in data

---

[2] *See*, *e.g.*, *Thompson Med. Co.*, 104 F.T.C. 648, 813 (1984), *aff'd*, 791 F.2d 189 (D.C. Cir. 1986); *Daniel Chapter One*, 2009 WL 5160000 at *25–26 (F.T.C. 2009), *aff'd*, 405 Fed. App'x 505 (D.C. Cir. 2010) (unpublished opinion), *available at* 2011-1 Trade Cas. (CCH) ¶ 77,443 (D.C. Cir. 2010); *POM Wonderful, LLC*, 155 F.T.C. 1, 55–60 (2013), *aff'd*, 777 F.3d 478 (D.C. Cir. 2015), *cert. denied*, 136 S. Ct. 1839, 194 L. Ed. 2d 839 (2016); *FTC Policy Statement Regarding Substantiation*, 104 F.T.C. 839, 840 (1984) (appended to *Thompson Med. Co.*, 104 F.T.C. 648 (1984)).
[3] *See Guides for the Use of Environmental Marketing Claims*, 16 C.F.R. § 260.2 (2019), https://www.ecfr.gov/cgi-bin/text-idx?SID=bd96b2cdcd01f7620d43e50a9d1d8cec&mc=true&node=se16.1.260_12&rgn=div8; *Dietary Supplements: An Advertising Guide for Industry,* https://www.ftc.gov/tips-advice/business-center/guidance/dietary-supplements-advertising-guide-industry.

security cases, based on the Eleventh Circuit opinion, feedback we received from our December hearing on data security, and our own internal discussion of how our orders can create better deterrence of future misconduct, using our existing tools.

One of the reasons I support comprehensive data security and privacy legislation is that such legislation could limit the impact of competing court opinions by directly empowering the FTC to require reasonable data security and privacy practices.

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

Response. I support strong comprehensive privacy legislation that would (1) empower the FTC to seek significant monetary penalties for privacy violations in the first instance; (2) give the FTC APA rulemaking authority, to allow us to craft flexible rules that reflect stakeholder input and can be periodically updated to keep up with technological developments; and (3) repeal the common carrier and nonprofit exemptions under the FTC Act to ensure that more of the entities entrusted with consumer data are held to a consistent standard. Moreover, I support an increase in resources and personnel to enable the FTC to use these enforcement tools effectively.

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. The Commission's 6(b) investigative authority is a critical tool that the Commission can use to increase its understanding of industries and markets in order to inform both our competition and consumer protection policy and enforcement agendas. There are many issues in the technology arena that could be the subject of a 6(b) study, and I would support such an effort.

Responses to Written Questions Submitted by Honorable Jerry Moran to Rebecca Slaughter

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. Yes. The FTC has the experience and expertise to enforce new comprehensive privacy legislation—and the demonstrated dedication to consumers to do so effectively. The FTC's dual missions demand that we think critically about the impact of regulations and enforcement on both consumers and the competitive marketplace, which will be valuable in executing whatever framework Congress passes.

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. The Commission is always looking for ways to use existing resources more efficiently, but additional resources would be put to good use and help us to do more to further our competition and consumer protection missions. With respect to our merger enforcement efforts, economic and other experts are necessary to support investigations and bring litigation. As larger and larger mergers come before the Commission and complexity of investigations increase, the cost of outside experts becomes a greater resource burden. Resource constraints can require the agency to make difficult tradeoffs between litigating a case to achieve the optimal result and settling for a good but imperfect resolution.

Competition in the technology industry must be closely monitored and the Commission is well equipped to examine fast-moving high-technology markets. However, I think that creating a Bureau of Technology would be useful for centralizing technological expertise and more

regularly deploying technologists to assist in both competition and consumer protection investigations. As you know, there continues to be some overlap between competition and consumer protection issues and the Commission should always be mindful of the fact that what we do in the competition arena could impact our consumer protection mission and vice versa.

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. Yes, coupled with effective law enforcement, efforts to empower our senior consumers to recognize and avoid scams are invaluable. The FTC works closely with multiple federal, state, and private partners to increase awareness about frauds that target our seniors, and we have developed our own *Pass It On* campaign to share preventative information about frauds and scams with older adults.

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. Financial injury describes harm that can be quantified, such as lost money, time, or opportunity. When we talk about physical injury, that covers harms arising from increased risks to an individuals' health or safety, including their mental and emotional health. Reputational injury involves disclosure of private facts about an individual, which damages the individual's reputation. Finally, unwanted intrusion into the sanctity of people's homes, communications and intimate lives also constitute serious harms. Outside of lost dollars, quantifying appropriate relief to address these serious harms can present enforcement challenges that would be eased by consumer privacy legislation that imposed money penalties for privacy violations.

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. When the Commission brings an action sounding in its unfairness authority under Section 5 of the FTC Act, we can only challenge an act or practice that "causes or is likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves and not outweighed by benefits to consumers or to competition." The FTC does not, however, need to engage in this specific inquiry when it proceeds under its deception authority pursuant to Section 5 of the FTC Act. For example, when a company makes promises to

consumers about how it will collect, store or use consumer data and breaks those promises, the FTC need not engage in any balancing inquiry to bring an enforcement action.

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. To the extent that federal regulation would be more permissive in its treatment of de-identified data, I would urge careful consideration to ensure that data cannot be re-linked to individuals. For example, I would point to the formulation used in the EU General Data Protection Regulation ("GDPR"), which makes clear that "anonymization" of personal data refers to de-identified data for which direct and indirect personal identifiers have been removed and steps have been taken to ensure that the data can never be re-identified.

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.[4] 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

---

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

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.

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.[5]

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[6] and a public expo that allowed companies offering call blocking and call labeling services to showcase their products for the public.[7] 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. Under current law, the FTC generally cannot obtain civil penalties—in other words, money—for first-time security or privacy violations. This means that, in order to be financial liable for data security or privacy violations, a company often must violate the law, be pursued by the Commission and put under order, and then violate the law again. I believe this under-deters problematic data security and privacy practices. If Congress were to give us the authority to seek civil penalties for first-time violators, better deterrence would be achieved. As to APA rulemaking authority, the Commission would benefit from such authority in the areas of data

---

[5] 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.
[6] 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.
[7] 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.

security and privacy. Rulemaking authority will ensure that the FTC can enact rules, with notice and comment and consistent with Congressional direction, and amend them as necessary to keep up with technological developments. For example, in 2013, the FTC was able to use its APA rulemaking authority to amend its Rule under the Children's Online Privacy Protection Act to address new business models, including social media and collection of geolocation information, that were not in place when the initial 2000 Rule was promulgated. As to nonprofits and common carriers, news reports are filled with breaches affecting these sectors (e.g., the education sector), and the FTC does not currently have jurisdiction over them. Giving the FTC jurisdiction over these entities for purposes of enforcing data security and privacy laws will create a level playing field and ensure that these entities are subject to the same rules as other entities that collect similar types of data.