**Additional Questions for the Record**

**Subcommittee on Consumer Protection and Commerce**
**Hearing on**
**"Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security"**
**May 8, 2019**

**The Honorable Joseph J. Simons, Chairman**
**The Federal Trade Commission**

**The Honorable Jan Schakowsky (D-IL)**

1. **Expert witnesses play an integral role in the Federal Trade Commission's (FTC) enforcement of both competition and consumer protection laws, particularly in complex mergers or technical matters concerning privacy and data security. The FTC's FY2020 Budget Justification states that the Commission faces significant resource challenges due to the rising costs of expert witnesses' contracts.**

    a. **On average, how much does the FTC spend on expert witnesses in an individual case?**

    b. **How much does the FTC spend on expert witnesses per year?**

    c. **By how much have the costs of expert witnesses increased during the past 10 years?**

    d. **Has the FTC ever chosen not to pursue an enforcement action due to the prohibitive costs of expert witnesses?**

Thank you for your attention to this important issue. There are some complexities associated with our expert witness engagements, which we would like to clarify for the Subcommittee. We caution that reliance on average numbers over time may present a somewhat inaccurate view of the facts on the ground, given that our enforcement work may result in wide year-to-year variances in spending. Given some significant differences between competition and consumer protection cases, this response breaks out information separately for each of our two enforcement missions.

Competition Cases

When a competition case goes to litigation (versus settlement or closing), expert witness costs typically increase exponentially for that matter. As a result, the agency's annual expert witness costs for competition matters in a given fiscal year are largely a function of the number and types of competition cases the Commission must litigate during the course of that year. Since each additional litigated case may lead to millions of dollars in additional expert fees, even very small changes in the total number of competition cases per year can have a dramatic impact on the

agency's overall spending on expert fees. Although most of our cases ultimately settle, the total number of litigated cases can vary widely year to year.

Unfortunately, the agency has a limited ability to control this primary driver of our expert costs. This is particularly true with respect to merger matters, where outside parties dictate the volume, nature, and timing of their deals. The Commission votes out a complaint when it has reason to believe that a competition enforcement action is in the public interest. Post-vote, the course of litigation (and possible settlement) is determined in large part by the defendants and, of course, the judge or judges. Among other factors, defendants may choose to retain one or more experts of their own, which can affect our expert strategy.

In general, we have observed that the kinds of experts qualified for this kind of work are becoming more expensive. In an increasingly data-rich world, each case requires more of an expert's time, and more support resources to process data and increasingly large volumes of documents. Our expert budget is depleted not only by higher prices per hour worked, but also by the need for experts to spend more time preparing for each case, and the need for more support resources to manage each case.

On the competition side, we have determined that the range of total expert costs for cases that are fully litigated (meaning a preliminary injunction, administrative hearing on the merits or both) in the last five years is $583,100 - $6.90 million.

The remaining, requested data points for our competition cases are as follows:

| Fiscal Year | Expert Spending* |
|---|---|
| 2008 | $3.05 million |
| 2009 | $3.40 million |
| 2010 | $3.16 million |
| 2011 | $2.97 million |
| 2012 | $2.09 million |
| 2013 | $2.98 million |
| 2014 | $4.84 million |
| 2015 | $10.03 million |
| 2016 | $12.21 million |
| 2017 | $11.46 million |
| 2018 | $15.80 million |
| **Some years' expenditures may change due to ongoing work* | |

To date, the Commission has managed allocated funds to pay the expert witness fees needed to pursue vigorous competition enforcement on behalf of consumers. We are, however, increasingly concerned about our ability to continue to do so.

Consumer Protection Cases

Average expert cost per case: Between FY16 and FY18, the Commission filed an average of 71 consumer protection cases (mostly in federal court) per year, spending approximately $30,000 per case on expert witness contracts. The Commission uses experts in approximately 44 consumer protection matters per year, spending an average of approximately $49,000 on expert witness contracts in each of those cases.

Total yearly expert costs: Between FY16 and FY18, the Commission spent approximately $2.16 million on expert witness contracts for consumer protection cases per year, and is on track to obligate $2.28 million during FY19.

Expert spending over past 10 years: The Commission's expert spending on consumer protection cases has remained steady over the past 10 years. In FY 2008, the Commission expended approximately $2.07 million on expert contracts in consumer protection cases, and is on track to obligate $2.28 million during FY19.

2. **Since announcing the Hearing on Competition and Consumer Protection in the 21st Century, the FTC has held 13 hearings examining topics ranging from the FTC's vertical merger policies to privacy and data security. Some critics have observed that many of the panelists at these hearings, particularly economists, have significant financial ties to large corporations that are regulated by FTC, including Facebook, Google, and Amazon. One report suggests that more than a third of the scholars participating in the FTC's hearings have financial ties to Google. I am concerned by these criticisms because it suggests that the FTC is not hearing from unbiased points of view at these hearings.**

    a. **Does the FTC require panelists before appearing as an expert at FTC hearings or workshops to disclose financial ties to industry? If so, what are those requirements?**

    b. **How many panelists at the FTC's Hearings on Competition and Consumer Protection in the 21st Century disclosed financial ties to entities within the FTC's jurisdiction?**

    c. **Did the FTC publicize any such financial ties before the hearings, and, if not, why not?**

The FTC has taken significant steps to feature a wide variety of perspectives during the hearings. We have invited legal and economic academics, legal and economic consultants, public interest groups, public advocacy groups, and representatives of businesses and industries to our hearing sessions. By the time the hearings conclude on June 12, we will have hosted 393 unique non-FTC participants for 23 days of public hearings.

During hearings and workshops, the FTC generally asked panelists the following two questions:

1. Whether any third party funded or otherwise provided financial assistance for the research/analysis/commentary you will present at the hearing? If yes, who?

2. Whether any third party will compensate you for your participation at the hearing or otherwise provide financial assistance for your participation (e.g., reimburse your travel expenses)? If yes, who?

If a panelist answers yes to either question, we include that information and the name of the third party within the bios that we publish for each hearing. In addition, if a panelist is currently working for a corporation, we include that information in their bio as well. Bios and information are available on our website.

We have sought public input and, to the greatest extent possible, facilitated informed comments from a wide range of interested parties. For example, before each hearing, we have released an agenda, list of participants, and a list of specific questions designed to solicit comments. The public comment period has been open before each hearing, allowing commenters to raise issues for discussion at the public session. The comment period has also extended well beyond the date of each specific hearing, to allow interested parties to comment on the discussion at the public session. We stream each hearing session live, and place a video of the hearing session on our website for those who could not attend or watch live. We also release a transcript of each hearing shortly after conclusion of a session. We have, to date, received close to 900 unique comments on our hearings topics. The FTC posts all germane comments online shortly after we receive them, allowing the public to comment on points raised in the public comments. The public comments will receive the same review, scrutiny, and consideration as the comments and discussion at our hearings. There are no restrictions on who can comment, and I believe the public written comments are as important and valuable as the commentary at our hearing sessions. We have also consulted the substantial body of academic literature available on each topic we have taken testimony on, in preparation for each hearing.

The Commission and its staff regularly review arguments and advocacy of parties, persons, and interest groups who appear before us on enforcement and policy matters. Often, they do not disclose their source of funding, their direct or indirect interest in the matter they bring before us, or how they (or their clients or funders) might benefit from the outcome they seek. In those situations, we carefully evaluate the information and arguments on the merits. We will do the same here.

3. **The FTC's Bureau of Economics plays an important role in both the FTC's competition and consumer protection enforcement. But reports indicate that the Bureau of Economics approaches privacy and data security cases with skepticism, based on a view that few privacy or data security practices cause injury, or that consumers do not meaningfully engage with privacy policies (and therefore cannot be deceived by them).**

    a. **How does the Bureau of Economics participate in the FTC's privacy and data security matters? To what extent does the Bureau of Economics influence whether a privacy or data security investigation continues?**

    b. **Has the Bureau of Economics dissented from or otherwise opposed any of the FTC's privacy enforcement matters in the past 5 years and, if so, how many?**

The Bureau of Economics supports the FTC's privacy and data security work by providing high quality, up-to-date economic analysis and advice. The Bureau of Economics provides the Commission with independent economic analysis of the harms and potential harms stemming from alleged Section 5 violations. The Bureau of Economics continues to develop innovative solutions to deal with the known difficulties of measuring the harm associated with privacy and data security practices.

The Bureau of Economics reviews every complaint or settlement recommendation that the Bureau of Consumer Protection makes on privacy and data security matters, as they do in all enforcement matters. The Bureaus discuss these matters at the staff and management level. In some instances, the Bureau of Economics may persuade the Bureau of Consumer Protection to modify, add, or drop certain complaint allegations or theories of liability. The Bureau of Consumer Protection then presents its final recommendation to the Commission, and the Bureau of Economics provides a separate recommendation memorandum to the Commission.

In the past five years, the Bureau of Economics has disagreed with three of the Bureau of Consumer Protection's privacy and data security case recommendations (out of approximately 60 total recommendations). In a few other cases, the Bureau of Economics has supported BCP's recommended action, but raised issues about particular proposed complaint allegations.

4. **On June 11, 2019, the FTC will hold a workshop on online event tickets. I have heard reports of a number of consumer protection issues concerning online event tickets that raise serious concerns and I hope the FTC will consider addressing these issues during its workshop. For example, I have heard concerns that primary ticket platforms have begun forcing purchasers to disclose personally identifiable information by creating an account with the primary ticket seller to use a ticket, even when tickets are resold on a secondary market. I have also heard complaints about primary ticket sellers that hold tickets back from the market pursuant to agreements with venues, artists, or other partners. In addition, I have received complaints about primary ticket vendors putting technological restrictions on the transfer of tickets, which can prevent ticket holders from reselling or giving away tickets if they cannot attend the event.**

    a. **Will the FTC examine these issues at its upcoming hearing on online event tickets?**

Yes, the June 11 Online Event Ticketing Workshop will examine the issues that you raise and their possible impact on consumers in the online event tickets marketplace.

    b. **Has the FTC received similar complaints from consumers?**

The most common consumer complaints we receive about online event ticketing concern either hidden or inadequately disclosed ticketing fees in the primary and secondary markets, or reports that ticket resellers misled consumers to believe they were purchasing tickets from the venue or authorized seller at face value (when in fact they were purchasing tickets from resellers at a significant markup). The Commission has also received several thousands of consumer comments in connection with the upcoming ticketing workshop. Those comments

overwhelmingly concern hidden or inadequately disclosed ticketing fees and/or the high cost of such fees. While the FTC may also have received consumer complaints or comments regarding the practices you outline, they do not appear to be as prevalent.

**c. Do you agree that, if true, these practices raise concerns about unfair or deceptive practices in the market for online event tickets?**

These practices may raise questions about transparency and consumer understanding in the online event tickets marketplace; however, it is unclear whether requiring ticket buyers to provide personally identifying information, holding back tickets for later sale, or restricting the transfer of tickets would be unfair or deceptive acts or practices under Section 5 of the FTC Act.

**The Honorable Bobby L. Rush (D-IL)**

1. **In 2014, the Federal Trade Commission (FTC) published a report called "Data Brokers: A Call for Transparency and Accountability" that shed light on the secretive world of data brokers that buy and sell vast amounts of consumer personal information, often entirely behind the scenes. The FTC's report called on Congress to pass legislation that would require data brokers to be more transparent and give consumers the right to opt-out, among other things.**

    **a. Do you still agree that Congress should pass legislation addressing data brokers?**

The current Commission has not taken a position on data broker legislation. I support federal privacy and data security legislation that would give the Commission authority to seek civil penalties for first-time privacy and data security violations; conduct targeted APA rulemaking; and exercise jurisdiction over common carriers and non-profit entities.

2. **While innovation in the tech industry is having a tremendous impact on our economy and the lives of everyday Americans, it is also creating new challenges in protecting consumers and competitive markets. I have heard reports of certain online platforms giving their subsidiary businesses preferential treatment over their competitors.**

    **a. Are you looking into anti-consumer and anti-competitive behaviors of this nature?**

    **b. In your opinion, does the FTC currently have the authority and capacity to curtail this behavior?**

As more and more of the nation's commerce takes place on online platforms, the operation of these platforms has received increased scrutiny by both the public and the antitrust agencies. I believe the FTC has many of the tools it needs to protect consumers online, although I have called for Congress to give the FTC the authority to seek civil penalties for initial privacy violations, which would create an important deterrent effect. Moreover, I believe consumers

would benefit if the FTC had broader enforcement authority to take action against common carriers and non-profits, which it cannot currently do under the FTC Act. That said, the FTC is vigilant in its oversight of the internet economy, and we will not hesitate to take strong and appropriate action against any act or practice that violates any statute we enforce.

The Bureau of Competition recently announced the creation of a Technology Task Force ("TTF") that will enhance the Commission's antitrust focus on technology-related ecosystems, including technology platforms as well as markets for online advertising, social networking, mobile operating systems, and apps. The TTF will monitor competition in U.S. technology markets, investigate any conduct in these markets that may harm competition, and, when warranted, take actions to ensure that consumers benefit from free and fair competition.

The FTC does not publicly comment on pending law enforcement investigations. However, I can provide some guidance as to the applicable legal standards under current law.

As a threshold matter, it is important to appreciate that there are no special antitrust rules for online platforms. The same core antitrust laws and principles that apply generally across the economy apply to online platforms as well. This includes the laws relating to monopolization. Whether a firm is an online platform or a company that operates brick-and-mortar stores, if the firm has monopoly power or a dangerous probability of acquiring such power, the firm is subject to the same prohibitions under the U.S. antitrust laws: it cannot engage in anticompetitive conduct that tends to contribute to the acquisition or maintenance of monopoly power and lacks a procompetitive efficiency justification.

If FTC staff were to analyze an allegation that an online platform had violated the antitrust laws by discriminating against competitors, FTC would apply the test described above. To evaluate whether an online platform might have monopoly power, we would consider the online platform's share of the relevant market (or markets) in which it competes, as well as other factors (such as the existence and magnitude of barriers to entry). If a platform with monopoly power were to extend some form of preferential treatment to its own business units in a way that was alleged to contribute to the improper acquisition or maintenance of monopoly power, that conduct would be analyzed through a careful and fact-specific inquiry that considered the nature of the conduct, the extent to which it excluded competition, and any efficiency justifications.

As with most antitrust analysis, the conduct you describe would be neither automatically legal or automatically illegal; the specific nature of the conduct, and its positive and negative effects on competition and consumers, would matter very much. The U.S. antitrust laws do not impose a universal duty to deal with one's competitors on the same terms as with other divisions of one's own company. The antitrust laws do, however, recognize that certain forms of adverse treatment of competitors can, under appropriate circumstances, give rise to antitrust liability when the conduct contributes to the wrongful acquisition or maintenance of monopoly, and thereby harms competition. The FTC's talented and hard-working staff invest considerable time and energy to identify conduct that unlawfully harms competition and consumers in all areas of the economy, including online platforms, and will continue to do so.

3. **As all of you know, robocalls are extremely burdensome on consumers and every effort needs to be taken to ensure that consumers are not being taken advantage of by these unscrupulous actors. I am also concerned by the reports I have heard that robocalls are now being used by online contact lens retailers to usurp the verification of contact lens prescriptions, placing consumers at an even greater risk of receiving the wrong Class II or III medical devices.**

    a. **Do you agree that efforts need to be taken to update the passive verification process?**

When Congress enacted the Fairness to Contact Lens Consumers Act ("FCLCA"), it determined that passive verification was necessary to balance the interests of prescription portability and consumer health. Congress was aware that, in some instances, passive verification could allow sellers to sell contact lenses based on an invalid or inaccurate prescription, and that this could potentially lead to health risks. In the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM"), the Commission proposed several changes to improve the passive verification process. The Commission proposed that sellers who use automated telephone verification messages would have to: (1) record the entire call and preserve the complete recording; (2) begin the call by identifying it as a prescription verification request made in accordance with the Contact Lens Rule; (3) deliver the verification message in a slow and deliberate manner and at a reasonably understandable volume; and (4) make the message repeatable at the prescriber's option. This proposal would enable prescribers to better fulfill their role as protectors of patients' eye health because prescribers cannot correct and police invalid, inaccurate, and expired prescriptions if they cannot comprehend a seller's verification request.

Additionally, the Commission proposed changes that would increase patients' access to their prescriptions, maintain patient choice and flexibility, and potentially reduce the number of verification requests. Under the proposal, a prescriber, with the patient's verifiable affirmative consent, has the option to provide the patient with a digital copy of the prescription in lieu of a paper copy. Moreover, although the Rule has always required that prescribers, upon request, provide any person designated to act on behalf of the patient with a copy of the patient's valid contact lens prescription, the Rule did not prescribe a time limit within which this copy had to be provided. The Commission proposed requiring that a prescriber respond to requests for an additional copy of a prescription within forty business hours. To facilitate patients' ability to use their prescriptions, another proposed change would require sellers to provide a mechanism that would allow patients to present their prescriptions directly to sellers.

Finally, the Commission proposed amending the prohibition on seller alteration of prescriptions to address concerns about the misuse of passive verification to substitute a different brand and manufacturer of lenses. The proposal requires a seller who makes an alteration to provide a verification request to the prescriber that includes the name of a manufacturer or brand other than that specified by the patient's prescriber. There is a proposed exception if the patient entered that manufacturer or brand on the seller's order form or the patient orally requested it from the seller.

The Commission will consider comments received in response to the SNPRM and, if appropriate, make changes before issuing a final rule.

**b. Do you agree that robocalls need to be eliminated from use within the passive verification system?**

No, I do not agree with categorically eliminating the role of automated technology within the passive verification system. An effective verification process enables prescribers, when necessary, to prevent improper sales and allows sellers to provide consumers with their prescribed contact lenses without delay. The FCLCA expressly permits telephone communication for verification. It would be contrary to Congressional intent to prohibit the use of automated technology for the purpose of prescription verification. The Commission does not have empirical data showing the frequency of incomplete or incomprehensible automated telephone messages, or supporting a claim that a phone call with an automated message is necessarily less reliable than one with a live person. Rather, the evidence suggests that these calls can be an efficient method of verification. The Commission recognizes, however, the burden on prescribers and potential health risk to patients from incomplete or incomprehensible automated telephone messages. As described in response to question 3.a, the Commission has proposed changes to automated telephone messages that would improve the verification process.

**c. Could you support updating the Fairness to Contact Lens Consumers Act to eliminate robocalls and update the passive verification system to include secured emails and patient portals to verify and document contact lens prescription verification?**

I would not support categorically eliminating the role of automated phone call technology within the passive verification system. I do support clarifying that emails and portals would be acceptable mechanisms for prescription verification. Under the current Rule, a "seller may sell contact lenses only in accordance with a contact lens prescription for the patient that is: (1) Presented to the seller by the patient or prescriber directly or by facsimile; or (2) Verified by direct communication." 16 C.F.R. § 315.5(a). Because the Rule's definition of direct communication already includes electronic mail, a seller and a prescriber currently could use email during the verification process. In the December 7, 2016 Notice of Proposed Rulemaking ("NPRM"), the Commission made an initial determination that a portal could be used by a prescriber or a patient to "directly" present a contact lens prescription to a seller. The Commission will consider comments received in response to this initial determination and, if appropriate, make changes before issuing a final rule.

**4. In December 2016, the FTC issued a Notice of Proposed Rulemaking to update the Contact Lens Rule. As a part of this process, providers and manufacturers of contact lenses urged the FTC to require common-sense changes to the current contact lens market, including quantity limits and ways to update methods of communication under the passive verification process. The FTC responded by stating that there was insufficient evidence that consumers are buying excessive quantities of contact lenses and that it did not have the statutory authority to update the passive verification process.**

**a. Do you support efforts to ensure patient safety regarding the current proposed rulemaking process that will include patients only receiving contact lenses as prescribed under the valid prescription?**

The Commission does not believe patients should be able to purchase contacts without a valid prescription. The SNPRM's proposed changes improve patient access to contact lens prescriptions and address concerns with the passive verification requests and alterations by sellers.

**5. Last May, Rep. Michael Burgess (R-TX) and I led a letter to the FTC that laid out several concerns we have regarding the FTC rulemaking process around the Fairness to Contact Lens Consumers Act. In total, over 50 members of Congress signed this letter where we discussed the lack of enforcement action by the FTC to address the illegal sales of contact lenses and the burdensome new requirements on eye care providers.**

**a. Has the FTC investigated or independently audited any online sellers to determine the number of lenses provided to patients?**

The Commission has not audited online sellers to determine the number of lenses provided to patients.

**b. What enforcement mechanisms has the FTC used to ensure that sellers are not enabling the circumvention of state laws governing prescription renewal or harming patients by providing excessive numbers of contact lenses?**

In the NPRM, the Commission considered the issue of patients purchasing excessive quantities of contact lenses. Although concerned with anecdotal reports, the Commission concluded that the evidence did not show that the sale of excessive amounts of contact lenses is a widespread problem.[1] Furthermore, a prescriber who receives a verification request for an excessive amount of lenses can contact the seller to prevent the sale from being completed. Staff has investigated specific complaints of illegal sales related to excessive quantities. We will continue to monitor the marketplace, taking action against violations as appropriate.

**c. How often has the FTC acted on this important safety issue?**

As discussed in the response to question 5.b, the Commission does not believe that the evidence shows that excessive sale of contact lenses is a widespread problem. The Commission does, of course, recognize the importance of patient safety. Staff will continue to monitor the marketplace and, if appropriate, take action.

**6. Many businesses are increasingly dependent on digital platforms that they do not own or operate to connect with customers.**

[1] NPRM at 88549-50; *see also* Vision Council, U.S. Optical Market Eyewear Overview 13 (2018), https://www.ftc.gov/sites/default/files/filefield_paths/steve_kodey_ppt_presentation.pdf (noting that 82% of contact lens users had an eye exam within the last 12 months and over 95% had an exam within the last two years).

**a. With current statutory authorities in mind, what can be done to protect consumers if companies that operate these platforms offer subsidiary business products and restrict or disadvantage competitors with similar businesses on these platforms? What is the FTC doing to curtail it?**

**b. One example of how a platform operator might harm consumers is by prohibiting businesses from communicating with their customers through that platform. Do you believe that this sort of behavior must be addressed and, if so, does the FTC currently have the statutory authority to do so?**

Please see the answer to question 2.

**7. It has been brought to my attention that the leading internet browser has been considering a major change in what type of information is available to consumers in their product, reducing the available information that consumers use to defend themselves against a host of online threats like phishing and content spoofing.**

**a. As the agency charged with protecting our nation's consumers and enforcing our data privacy laws, do you have concerns about what this practice means for consumers and their data privacy and security?**

**b. Have you discussed this issue with the browsers or asked them to explain their changes and how they will impact consumer safety online? If not, do you intend to?**

I understand your question to refer to how browsers display certain digital certificates in their user interface. When properly validated, digital certificates serve as proof that consumers are communicating with an authentic website and not an imposter. They also serve to encrypt traffic between a consumer's browser and a site's web server.

In May 2018, Google announced that it would change its user interface in its Chrome browser to remove certain indicators of the presence of an expensive digital certificate – called an extended validation certificate – such as green text and a padlock icon. I have not discussed these changes with Google. Consumers' secure online experiences depend on many factors, and the ecosystem continues to evolve quickly. I do not believe that the Commission should promote one type of certificate over another, or prescribe how certificates should be displayed in user interfaces.

The Commission is committed to promoting consumer safety online. In addition to our enforcement work, detailed in the Commission's written testimony, we engage in extensive consumer education, examples of which you may find here: https://www.consumer.ftc.gov/articles/0009-computer-security.

**The Honorable Cathy McMorris Rodgers (R-WA)**

1. **Chairman Simons, the FTC has existing rulemaking authority but is now asking Congress for additional APA rulemaking authority. Please answer the following questions about the Commission's existing rulemaking authority:**

    a. **When was the most recent opened rulemaking proceeding initiated? Please include the statutory authority permitting or directing the rulemaking.**

    b. **When was the most recent completed rulemaking proceeding completed? Please includes the statutory authority permitting or directing the rulemaking.**

The FTC opened its most recent proceeding to promulgate a new substantive rule in November 2018.[2] The 2018 Economic Growth, Regulatory Relief, and Consumer Protection Act, among other things, required that nationwide consumer reporting agencies provide free electronic credit monitoring services to active duty military consumers. It also required the FTC to issue regulations clarifying the meaning of certain terms used in the Act, as well as clarifying what constitutes appropriate proof that an individual is an active duty military consumer.[3]

In addition, the FTC reviews all of its existing rules periodically to seek information about their costs and benefits and their regulatory and economic impact. Most recently, in March 2019 the FTC announced a regulatory review of, and invited public comment on, the Franchise Rule.[4] The Franchise Rule makes it an unfair or deceptive act or practice for franchisors to fail to give prospective franchisees a Franchise Disclosure Document providing specified information about the franchisor, the franchise business, and the terms of the franchise agreement; it also prohibits related misrepresentations by franchise sellers. The Commission issued the original Franchise Rule in 1978 pursuant to its authority under Section 5 of the Federal Trade Commission Act to proscribe unfair or deceptive acts or practices.

In terms of completed new rules (as opposed to amendments of existing rules), the most recent new substantive rule issued by the Commission was the Business Opportunity Rule.[5] The Business Opportunity Rule governs disclosure requirements and prohibitions for business opportunities. The legal basis for the rule is Section 18 of the FTC Act, 15 U.S.C. § 57a, which authorizes the Commission to promulgate, modify, and repeal trade regulation rules that define with specificity acts or practices in or affecting commerce that are unfair or deceptive within the meaning of Section 5 of the FTC Act.

In the first half of 2019, the FTC completed its regulatory review for a number of rules and closed out those rulemaking proceedings. For example, the FTC amended its trade regulation rule concerning the labeling and advertising of home insulation to clarify, streamline, and

[2] *See* 83 Fed. Reg. 57693 (Nov. 16, 2018).
[3] *See* Pub. L. No. 115-174, § 302(d).
[4] *See* 84 Fed. Reg. 9051 (Mar. 13, 2019).
[5] *See* 72 Fed. Reg. 76815 (Dec. 8, 2011).

improve existing requirements; retained without modification the trade regulation rule concerning preservation of consumers' claims and defenses; and retained without modification its rule implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM").[6] Both of the trade regulation rules were issued under Section 18 of the Federal Trade Commission Act, 15 U.S.C. § 57a. The CAN-SPAM rule was issued under 15 U.S.C. §§ 7701-7713, which provides for both mandatory rulemaking and discretionary regulations concerning certain statutory definitions and provisions.

2. **Chairman Simons, currently, does the Commission utilize an expert witness for data privacy enforcement actions?**

    a. **If yes, please detail the average cost of an expert witness used for data privacy enforcement actions, including any factors that could change the cost.**

3. **Chairman Simons, currently, does the Commission utilize an expert witness for data security enforcement actions?**

    a. **If yes, please detail the average cost of an expert witness used for data security enforcement actions, including any factors that could change the cost.**

In answer to questions 2 and 3, the Commission currently employs five technologists, three of whom work full time on privacy and data security matters. These technologists provide expert assistance on privacy and data security cases, for example, by helping attorneys draft discovery requests, participating in meetings with opposing parties, assisting staff in better understanding technical issues, and reviewing pleadings for technical accuracy. In addition, the Commission currently employs a consulting expert on data security, who provides advice regarding numerous data security investigations per year. He charges $300 per hour, and we typically use a few hours of his time every month.

The Commission also retains consulting and testifying experts for specific litigation matters. In its three litigated data security cases, the Commission has spent respectively about $2 million, $250,000, and $400,000 on experts, though the third case is not yet complete. Depending on the case, the Commission also would need experts on claim interpretation, who typically charge $250 per hour; experts on surveys and copy tests, who typically charge $675 per hour; experts on harms suffered by consumers, who have charged between $400 and $675 per hour; and experts on data security, who have charged between $150 and $550 per hour.

4. **Chairman Simons, how are Bureau of Economics staff utilized in data security and data privacy cases within the Bureau of Consumer Protection? Please give specific examples of action items in an enforcement case assigned to the Bureau of Economics staff.**

[6] *See* 84 Fed. Reg. 20777 (May 13, 2019); 84 Fed. Reg. 18711 (May 2, 2019); 84 Fed. Reg. 13115 (Apr. 4, 2019).

The Bureau of Economics reviews every complaint or settlement recommendation that the Bureau of Consumer Protection makes on privacy and data security matters, as they do in all enforcement matters. The Bureau of Economics provides a separate recommendation memorandum to the Commission. In some instances, the Bureau of Consumer Protection requests more specific input from staff economists. For example, staff economists may assist Bureau of Consumer Protection staff with drafting discovery requests aimed at determining the amount of harm caused by a particular practice; analyzing, categorizing, and creating statistical samples of consumer complaints; and developing surveys, studies, and/or copy tests, either with Bureau of Consumer Protection staff as part of an investigation or with outside experts during litigation.

**5. Chairman Simons, with respect to violations of an FTC consent order, what authority does the Commission have to hold company executives personally liable for company acts or practices the Commission determines to violate such order?**

**a. Please identify the specific statute, rule, or regulation that grants the Commission such authority.**

Rule 65(d)(2) of the Federal Rules of Civil Procedure explicitly states that federal court orders bind a party's officers, agents, servants, employees and attorneys. To prevail against a non-party to an order, the Commission must prove that defendants violated a valid, clear, and unambiguous order where they had notice of the order and the ability to comply.[7] Rule 65(d) applies equally to the Commission's administrative orders.[8]

**6. Chairman Simons, with respect to Section 5 of the FTC Act, what authority does the Commission have to hold company executives personally liable for company acts or practices the Commission determines to violate Section 5?**

**a. Please identify the specific statute, rule, or regulation that grants the Commission such authority.**

Numerous circuit courts have held that an individual officer, director, or employee may be held liable under the FTC Act for a company's unlawful acts or practices, if the FTC proves the necessary level of involvement. Specifically, individual liability for injunctive relief can be established by showing that the individual defendant participated directly in the unlawful practices or had authority to control them. Individual liability for monetary relief can be established by showing that the individual defendant, in addition to meeting the standard for injunctive relief, had actual knowledge of the unlawful conduct, was recklessly indifferent to its unlawfulness, or had an awareness of a high probability of illegality and intentionally avoided learning the truth.[9]

---

[7] *Angiodynamics, Inc. v. Biolitec AG*, 780 F.3d 420, 426 (1st Cir. 2015).

[8] *Reich v. Sea Sprite Boat Co.*, 50 F.3d 413, 417, (7th Cir. 1995) ("Long ago, however, the Supreme Court held that Rule 65(d) simply restates a norm of federal equity practice and therefore is equally germane to orders enforcing decisions of administrative agencies. *Regal Knitware Co. v. NLRB*, 324 U.S. 9, 14 (1945)."

[9] *See, e.g.*, *FTC v. Ross*, 743 F.3d 886, 892-93 (4th Cir. 2014); *FTC v. Direct Mktg. Concepts, Inc.*, 624 F.3d 1, 12 (1st Cir. 2010); *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1202-07 (10th Cir. 2005); *FTC v. Publ'g Clearing*

7. **Chairman Simons, with respect to trade regulation rules prescribed by the Commission under Section 18 of the FTC Act, what authority does the Commission have to hold company executives personally liable for company acts or practices the Commission determines to violate a trade regulation rule?**

    a. **Please identify the specific statute, rule, or regulation that grants the Commission such authority.**

When the FTC issues a trade regulation rule under Section 18 of the FTC Act, it does so in order to define with specificity acts or practices that are unfair or deceptive within the meaning of Section 5 of the FTC Act. Courts have held that the standard for liability of individual officers, directors, or employees that applies in Section 5 cases, discussed above in response to Question 6, also applies in cases brought to enforce trade regulation rules.[10]

8. **Chairman Simons, some stakeholders have raised concerns with companies naming products or features that arguably misrepresent the product's capability. For example, Tesla has a feature named "Autopilot" that arguably suggests their cars can operate fully autonomously without human intervention. The operation instructions include disclosures around the feature capabilities which are designed only to assist the driver and that the system requires active driver supervision. With respect to naming products that exceed the products capabilities, please answer the following:**

    a. **Does the FTC have any existing authority to address this concern? If so, please identify such authority.**

The FTC has authority to address product names that exceed the product's capability under Section 5 of the FTC Act, which generally prohibits "unfair or deceptive acts or practices in or affecting commerce."[11] As set forth in the FTC's *Deception Policy Statement*, the FTC considers an act or practice to be deceptive if it contains a representation or an omission of information that would be considered material to consumers and that would mislead consumers acting reasonably under the circumstances.[12] In addition, the Commission has long held that making objective claims without a reasonable basis for the claims constitutes a deceptive practice.[13] Whether or not a particular product name conveys a particular performance claim to consumers would be determined on a case-by-case basis. In some cases, extrinsic evidence may

---

*House, Inc.*, 104 F.3d 1168, 1170-71 (9th Cir. 1997); *FTC v. Gem Merch. Corp.*, 87 F.3d 466, 470 (11th Cir. 1996); *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 573-74 (7th Cir. 1989).

[10] *See, e.g., FTC v. Nat'l Bus. Consultants, Inc.*, 781 F. Supp. 1136, 1145 (E.D. La. 1991); *FTC v. Essex Marketing Group, Inc.*, No. 02-cv-3415, 2008 WL 2704918, at *4-6, (E.D.N.Y. July 8, 2008); *FTC v. Wolf*, No. 94-8119-CIV, 1996 WL 812940, at *8 (S.D. Fla. Jan. 31, 1996).

[11] 15 U.S.C. § 45.

[12] *See FTC Policy Statement on Deception, appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

[13] *FTC Policy Statement Regarding Advertising Substantiation*, 104 F.T.C. 839 (1984), appended to *Thompson Med. Co.*, 104 F.T.C. 648 (1984).

be needed to determine whether consumers acting reasonably would find a particular product name misleading.

**b. Could the Commission's deception authority be applied to review such cases?**

The Commission's Section 5 authority to prohibit unfair or deceptive practices extends to false or unsubstantiated advertising claims, including claims made through product names.[14]

**9. Chairman Simons, what are the limitations on the Commission's existing deception authority with respect to data privacy?**

**a. Please answer the same question above with respect to data security.**

In order to prove that a claim is deceptive under the FTC Act, the Commission must show that the claim has been made, that it is likely to mislead a consumer acting reasonably under the circumstances, and that it is material. Companies often make claims about privacy and data security in their privacy policies. Some defendants have argued that, because consumers do not typically read privacy policies, claims contained therein cannot be material, and therefore cannot be deceptive under the FTC Act. Although prior Commission statements and relevant case law are contrary to this argument,[15] the Commission likely will continue to face continued legal challenges on this issue.

**10. Chairman Simons, what are the limitations on the Commission's existing unfairness authority with respect to data privacy?**

**a. Please answer the same question above with respect to data security.**

Defendants in litigation have made several arguments as to the limitations of the FTC's unfairness authority in the areas of privacy and data security. Most of these arguments relate to the first element the FTC needs to prove in unfairness cases: that an act or practice "causes or is likely to cause substantial injury to consumers."[16] First, defendants have argued that certain non-financial and non-physical harms are not "substantial injury," based on legislative history stating that "emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."[17] Second, they have argued that, in order to prove that a practice is "likely" to cause substantial injury, the FTC must prove that injury is probable, or will occur with a 51% certainty. Third, defendants have argued that the FTC cannot prove that a

[14] *See, e.g., Brake Guard Prods., Inc.*, 125 F.T.C. 138 (1998) (Commission challenged claims that aftermarket brake product, "Brake Guard ABS," was an antilock braking system and provided the benefits of same; Commission order banned the use of the term "ABS" in connection with the product)

[15] *See FTC Policy Statement on Deception*, 103 F.T.C. 110, 174 (1984) (*appended to Cliffdale Assocs., Inc.*) (noting several categories of material claims, such as express claims, claims about the central characteristic of a product, and claims that the Defendant intended to make); *see also In the Matter of Novartis*, 1999 FTC LEXIS 63 *38 (May 27, 1999) ("Materiality is not a test of the effectiveness of the communication in reaching large numbers of consumers. It is a test of the likely effect of the claim on the conduct of a consumer who has been reached and deceived.").

[16] 15 U.S.C. 45(n).

[17] *See FTC Policy Statement on Unfairness*, 104 F.T.C. 949, 1070 (1984) (*appended to International Harvester).*

particular practice "caused" a given injury. For example, in a data breach case, it may be difficult to prove that a particular theft of a consumer's identity resulted from the specific breach at issue in the case.[18] The Commission has rejected each of these arguments,[19] and the Third Circuit in the *Wyndham* case has also confirmed that non-financial injury, such as the cost of people's time in dealing with a breach, is cognizable injury under the FTC Act.[20] Nonetheless, we continue to expend significant litigation resources on these issues.

**11. Chairman Simons, we know that small businesses have suffered in Europe since the implementation of GDPR, with some reports finding that investments in startups are down 40 percent. Do you have any suggestions for how can we guard against the same happening here with a federal privacy bill, including lessons learned from the public hearings on consumer protection issues in the 21st Century?**

Because the GDPR has been in effect for only a year, there is a limited basis upon which researchers and others might draw conclusions about potential effects that the GDPR has had on investments in startups. That said, the FTC's recent *Hearings on Competition and Consumer Protection in the 21st Century* did include discussion of research showing that, in the European Union, the number of venture capital technology deals and the average amount invested per deal declined in the first several months after the GDPR took effect.[21] Researchers have stated their intent to monitor to see whether those observations remain true on a longer-term basis, and whether they reflect correlation or causation. The FTC will keep abreast of such research.

**12. Chairman Simons, at the hearing, you indicated that a federal privacy bill should consider State Attorneys General enforcement. Please answer the following questions about state enforcement:**

**a. Do you agree that any state enforcement action of the federal law should be brought exclusively in federal court?**

**i. If yes, please explain.**

**b. Do you agree that the Commission should receive notice from a state prior to state enforcement of the federal privacy bill?**

**i. If yes, please explain.**

**c. Do you agree that the Commission should be able to intervene in any civil action brought by a state?**

**i. If yes, please explain.**

---

[18] *See, e.g.*, *LabMD, Inc. v. FTC*, Appellee's Initial Brief, 2017 U.S. 11th Cir. Briefs Lexis 14*, 10-11 (Feb. 9, 2017).
[19] Opinion of the Commission, *In re LabMD*, Docket No. 9357, 2016 FTC Lexis 128*, 59-60 (July 28, 2016).
[20] *FTC v. Wyndham Worldwide Corp., et al.*, 10 F. Supp. 3d 602, 621-22 (D.N.J. 2014).
[21] Jia, Jian and Jin, Ginger Zhe and Wagman, Liad, *The Short-Run Effects of GDPR on Technology Venture Investment* (May 31, 2019), https://ssrn.com/abstract=3278912 or http://dx.doi.org/10.2139/ssrn.3278912.

**d. Do you agree that if the Commission initiates a civil or administrative action on against the same defendant under the same circumstances of a state action, that the state action should be stayed pending resolution of the Commission's action?**

**i. If yes, please explain.**

I believe that the Children's Online Privacy Protection Act ("COPPA") provides a useful model for granting concurrent enforcement authority to state attorneys general. Under COPPA, state attorneys general can bring civil actions enforcing the law on behalf of their residents in federal district courts. The law requires that state attorneys general provide the Commission notice and a copy of the complaint before filing an action, unless doing so is infeasible. COPPA also gives the Commission the right to intervene in any civil action brought by a state and, if the Commission has instituted an action against a defendant, the law prohibits any state from filing a civil action against the same defendant for violating COPPA during the pendency of the Commission's action.

This model has been very successful. Multiple states, including Texas, New Jersey, and New York, have brought actions to enforce COPPA, which ultimately improves children's privacy. The other requirements of the COPPA statute help foster greater collaboration between the Commission and the states, and ensure that the law is interpreted in a consistent manner. I would be in favor of a similar approach in any future federal privacy law.

**13. Chairman Simons, in the 114th Congress this Committee, on a party line vote with Republicans voting for and Democrats voting against, reported the Data Security and Breach Notification Act of 2015 to the House Floor. Under that bill, the FTC would currently have first offense civil penalty authority for data security incidents like Equifax. Do you still agree, as you did during our oversight hearing held in July 2018, that the FTC would benefit from having civil penalty authority for violations of the Safeguards Rule?**

Yes. Financial institutions subject to the GLB Safeguards Rule often maintain highly sensitive personal information of consumers. Financial institutions that are subject to the Safeguards Rule and that do not comply should be subject to civil penalties for first-time violations.

**14. Chairman Simons, I appreciate your focus on whether our current consumer protection and competition laws are working as well as they should, especially in this digital world we now live in. That is why I was encouraged when you announced that you would be holding your 21st Century hearings on consumer protection issues, as well as creating the Technology Taskforce. Please answer the following with respect to the Technology Taskforce and hearings:**

**a. Please explain what the Technology Taskforce is and how you intend to utilize it's activities or findings with respect to data privacy and data security issues.**

**b. What is the status of the Technology Taskforce? How many FTEs are dedicated to the Taskforce?**

**c. Do you have any feedback from the 21st Century hearings you can share? If not, do you plan on producing any summary of findings from the hearings?**

**d. Do you have any feedback with respect to the Technology Taskforce you can share?**

The TTF will be a focal point for the Commission's efforts to further develop our legal and economic understanding of technology markets and promote effective antitrust enforcement in this area of the economy. It will provide a natural home for attorneys and economists with a technical background or with significant practical experience in relevant industries.

The primary focus of the TTF is to identify and investigate anticompetitive conduct (including consummated mergers) in markets in which digital technology is an important dimension of competition, such as online platforms, digital advertising, social networking, software, operating systems, and streaming services. Privacy and data security issues will continue to be handled by the Bureau of Consumer Protection, which has similar technology-focused components already in place. The Bureau of Competition will work closely with the Bureau of Consumer Protection on shared issues and concerns, especially in the context of investigations that raise related issues between privacy and data collection.

The TTF currently has 15 attorneys, with plans to hire two additional attorneys and a technologist soon. The TTF is supported by staff throughout the agency, including other technology experts and the Bureau of Economics. As there is no additional funding for personnel, all of the FTEs have come from within the FTEs allotted to the Bureau of Competition. The TTF staff is busy at work, and I expect them to move quickly to identify potential actions for the Commission.

The Commission's *Hearings on Competition and Consumer Protection in the 21st Century* have explored whether broad-based changes in the economy, evolving business practices, new technologies, and international developments might require adjustments to competition and consumer protection law, enforcement priorities, or policy. Several hearings have focused on the role of technology-based platform businesses. The Hearings and related public comments are helping the Commission obtain and evaluate a broad and diverse range of viewpoints from outside experts and interested persons about high-tech business practices.

**15. Chairman Simons, I understand there is an effort to modernize prescription release and delivery with patient portals and electronic health records (EHRs). There are some questions around the prescription verification process under the Contact Lens Rule. Are you soliciting comment about, and open to considering, updates to modernize the Contact Lens Rule to reflect how e-commerce has transformed the marketplace since it's origination?**

The Commission has proposed changes in the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM") to reflect advances in technology. Under this proposal, a prescriber, with the patient's verifiable affirmative consent, could provide the patient with a digital copy of the prescription in lieu of a paper copy. Additionally, the proposed Rule would require that sellers provide a mechanism to allow patients to present their prescriptions directly to sellers. Among other options, sellers could use email, text message, or file upload to obtain such prescriptions. Finally, in the December 7, 2016 Notice of Proposed Rulemaking, the Commission made an initial determination that a portal could be used by a prescriber or a patient to provide a contact lens prescription to a seller, which would allow the seller to complete the sale. The Commission will consider comments received in response to this initial determination and the SNPRM and, if appropriate, make changes before issuing a final rule.

**16. Chairman Simons, is the Commission aware of any other instances of verification by automated call for other self-administered class 2 and class 3 medical devices? If so, please list those other instances.**

The Commission is not aware of other instances where a self-administered class 2 or class 3 medical device can be verified with a medical provider using an automated telephone message.

**a. Please provide information on what percentages of verifications are filled through the following methods: fax, electronic means, personal live calls, or automated calls.**

The Commission does not have information about the percentage of verifications made through the various permissible methods.

**17. Chairman Simons, how many sellers does the Commission audit annually for verification compliance under the Contact Lens Rule?**

The Commission does not conduct annual audits of sellers or prescribers for compliance with the verification process. The Commission investigates sellers and prescribers based on complaints received and by monitoring the marketplace.

**a. How many of those audits have led to an enforcement action by the Commission?**

Since the Rule's passage, the Commission has taken law enforcement action against eleven contact lens sellers alleging violations of the Rule.[22] The settlement orders in these cases have provided injunctive relief that, among other things, prohibited the defendants from: selling contact lenses without obtaining a prescription from a consumer; selling contact lenses without

[22] *U.S. v. Lawrence L. Duskin*, No. 1:18-cv-07359 (N.D. Cal. Dec. 6, 2018); *U.S. v. Kim*, No. 1:11-cv-05723 (E.D.N.Y. Feb 7, 2012); *U.S. v. Royal Tronics, Inc.*, No. No. 0:11-cv-62491 (S.D. Fla. Jan. 27, 2012); *U.S. v. Thy Xuan Ho*, No. 1:11-cv-03419 (D. Minn. Dec. 27, 2011); *U.S. v. Gothic Lens, LLC*, No. 1:11-cv-00159 (N.D. Ga. Feb. 3, 2011); *U.S. v. Jokeshop, LLC*, No. 1:11-cv-11221 (D. Mass. Nov. 29, 2011); *U.S. v. Contact Lens Heaven, Inc.*, No. 0:08-cv-61713 (S.D. Fla. Dec. 3, 2008); *U.S. v. Chapin N. Wright, II*, No. 1:08-cv-11793 (D. Mass. Oct. 31, 2008); *U.S. v. BeWild, Inc.*, No. 2:07-cv-04896 (E.D.N.Y. Dec. 3, 2007); *U.S. v. Pretty Eyes, LLC*, No. 1:07-cv-02462 (D. Colo. Nov. 28, 2007); *U.S. v. Walsh Optical, Inc.*, No. 2:06-cv-03591 (D.N.J. Aug. 30, 2006).

verifying prescriptions by communicating directly with the prescriber; and failing to maintain records of prescriptions and verifications. In addition, the Commission has sent numerous warning letters to both sellers and prescribers who potentially violated the Rule. Staff will continue to monitor the marketplace and, if appropriate, take action.

**18. Chairman Simons, in March 2019, the FTC announced that it would be conducting a Section 6(b) study of certain Internet Service Providers. Does the Commission intend to conduct a similar study of consumer-facing content delivery services including social media services, sometimes referred to as "edge providers"?**

The Commission regularly uses its authority under Section 6(b) of the FTC Act, which allows it to conduct industry-wide studies. In the past few years alone, we have studied the practices of data brokers and mobile device manufacturers and, as you mention, we currently are undertaking a study of internet service providers. These types of studies are best suited to areas in which we can make apples-to-apples comparisons across a range of companies. We are considering further 6(b) studies in other industries.

**19. Chairman Simons, reports have surfaced that a Civil Investigative Demand (CID) has been issued by the Bureau of Competition to companies that run the largest automobile Dealer Management Systems (DMS) arising from an allegation that by improving the security of the DMSs, some companies are now technologically blocked from accessing them. These DMSs house and process dealership and manufacturer inventory, accounting, human resources and marketing information, and also contain financial, personal and sensitive data about consumer purchases and dealer services provided to consumers. As the FTC urge networks to secure personal data in testimony and guidance and other materials, is the Bureau of Competition having conversations with the Bureau of Consumer Protection about the various access issues that can arise with implementing security**

The agency does not publicly comment on the substance of any pending law enforcement investigation. I assure you that the Bureau of Competition and the Bureau of Consumer Protection regularly and appropriately work together on issues of common concern.

**The Honorable Robert E. Latta (R-OH)**

1. **Chairman Simons, the FTC has emphasized for years how important access to WHOIS data is to its online investigative and enforcement work. Domain name providers have begun limiting access to that data because of Europe's privacy law. The FTC's international consumer protection counsel has been documenting how that is hindering consumer protection and cyber security efforts, and the NTIA has called upon ICANN to solve this problem. How important is it that WHOIS access be restored as soon as possible to protect consumers and intellectual property?**

We believe it remains important for ICANN to develop a unified mechanism to enable those with legitimate interests—law enforcement, regulators, cyber security professionals, IP rights holders, and consumers—to obtain access to appropriate domain name registration (WHOIS) information. Contact information for domain name owners has long been one of the key building blocks in website investigations. The loss of ready access to this data due to EU privacy law developments has created obstacles and delays for those investigating illicit internet activities. For example, recent studies of more than 300 cybersecurity "first responders" and law enforcement investigators concluded that the masking of WHOIS information has impaired the ability to blacklist domains that transmit spam and expose internet users to online threats that could have been preemptively stopped, had WHOIS contact information remained available.[23]

We continue to cooperate with our foreign consumer protection and other enforcement counterparts to work towards a standard ICANN system to promptly and lawfully respond to requests for WHOIS information.

2. **Chairman Simons, we want companies of all sizes to protect consumer information, but we do not want new privacy obligations to crush small businesses and benefit big companies. In the 2012 FTC privacy report, the Commission grappled with this specific concern and excluded some small businesses from its recommendations. How do you think we should be addressing this concern?**

To the extent Congress is considering excluding small businesses from privacy legislation, we would suggest focusing not simply on the size of the company, but on the amount and sensitivity of the data the company collects. A company with few employees can collect highly-sensitive data of millions of consumers, and such a company should be subject to privacy rules. As you note, this is the approach the Commission took in its 2012 Privacy Report. We also took a similar approach in our recent Notice of Proposed Rulemaking on the GLB Safeguards Rule, where we proposed requiring all financial institutions to comply with general provisions requiring reasonable security, but suggested imposing more specific requirements on companies that collect data of more than 5,000 consumers.

3. **Chairman Simons, to date companies have failed to adequately explain to consumers how their information is collected, used, and often shared online. I**

[23] *See* Facts & Figures: Whois Policy Changes Impair Blocklisting Defenses, https://www.securityskeptic.com/2019/03/facts-figures-whois-policy-changes-impair-blacklisting-defenses.html.

**believe any federal privacy bill must increase transparency. Can you speak to why transparency is important?**

Transparency with respect to data collection, use, and sharing practices is important for multiple reasons. First, transparency helps consumers make informed decisions when choosing to provide their data to businesses whose practices align with the consumer's privacy preferences and expectations. Second, transparency promotes competition by enabling consumers to compare and contrast businesses' data practices and enabling businesses to compete based on their willingness and ability to meet consumers' preferences and expectations. Third, transparency promotes accountability by providing a basis for the FTC and other stakeholders to take action to hold businesses accountable if their actual practices do not comport with their claims. Finally, the process of publicly committing to certain data practices serves an important internal accountability function in making sure that company personnel examine and confirm the practices to which they are publicly committing.

4. **Chairman Simons, What data is being collected to determine the impacts of the GDPR in the United States? And does the FTC have a plan to collect data on the potential impacts of the CCPA? If that information is not being studied already, are there plans to study it?**

The FTC is continuing to collect public comments, including empirical research, until June 30, 2019, on the topics the FTC included in its recent *Hearings on Competition and Consumer Protection in the 21st Century*. The questions that the FTC has posted for public comment include:

- How do state, federal, and international privacy laws and regulations, adopted to protect data and consumers, affect competition, innovation, and product offerings in the United States and abroad?
- What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?
- Does the need for federal privacy legislation depend on the efficacy of emerging legal frameworks at the state level? How much time is needed to assess their effect?

The final hearing record will help inform future FTC plans to collect additional data to determine the impacts of the GDPR in the United States and the potential impacts of the CCPA as well as other existing or future privacy laws.

**The Honorable Michael C. Burgess (R-TX)**

1. **Chairman Simons, in December 2016, the FTC issued a Notice of Proposed Rulemaking announcing changes to the Commission's Contact Lens Rule. These changes included a new regulatory requirement for doctors to collect and maintain for 3 years a signed confirmation that a patient received their contact lens prescription. In addition, the proposal did not address illegal sales, including the filling of expired or incorrect prescriptions.**

   **On May 2, 2019, the FTC issued a Supplemental Notice of Proposed Rulemaking that kept the confirmation mandate, but allowed digital copies, and only required sellers to provide patient prescription information to prescribers in a slow and deliberate manner, without eliminating the automation of robocalls.**

   **Last Congress, Congressman Bobby Rush and I led a letter requesting the FTC reevaluate its 2016 proposed rulemaking, requesting the new rule limit the paperwork mandate and improve enforcement of existing provision to combat illegal sales.**

   a. **Can you describe why the FTC assesses the requirement to keep prescription confirmation records for 3 years is a necessary improvement upon the Contact Lens Rule?**

The Commission believes that maintaining records of prescription releases for three years will allow staff to investigate potential violations and, where appropriate, bring enforcement actions. The three-year period is consistent with other recordkeeping obligations in the Rule, and the FTC Act has a three-year statute of limitations for bringing enforcement actions pursuant to a rule violation.[24] Additionally, the Commission believes that some prescribers may already retain eye examination records for at least three years due to state requirements or may already keep customer sales receipts for financial recordkeeping purposes. The Commission will consider comments received in response to the May 28, 2019 Supplemental Notice of Proposed Rulemaking ("SNPRM") and, if appropriate, make changes before issuing a final rule.

   b. **Do you anticipate sellers maintaining the ability to exploit prescriber communication rules to fill prescriptions?**

When Congress enacted the Fairness to Contact Lens Consumers Act, it determined that passive verification was necessary to balance the interests of prescription portability and consumer health. Congress was aware that, in some instances, passive verification could allow sellers to sell contact lenses based on an invalid or inaccurate prescription, and that this could potentially lead to health risks. In the SNPRM, the Commission proposed several changes to improve the passive verification process. The Commission proposed that sellers who use automated telephone verification messages would have to: (1) record the entire call and preserve the

[24] 15 U.S.C. § 57b(d).

complete recording; (2) begin the call by identifying it as a prescription verification request made in accordance with the Contact Lens Rule; (3) deliver the verification message in a slow and deliberate manner and at a reasonably understandable volume; and (4) make the message repeatable at the prescriber's option. This proposal would enable prescribers to better fulfill their role as protectors of patients' eye health because prescribers cannot correct and police invalid, inaccurate, and expired prescriptions if they cannot comprehend a seller's verification request.

Additionally, the Commission proposed changes that would increase patients' access to their prescriptions, maintain patient choice and flexibility, and potentially reduce the number of verification requests. Under the proposal, a prescriber, with the patient's verifiable affirmative consent, has the option to provide the patient with a digital copy of the prescription in lieu of a paper copy. Moreover, although the Rule has always required that prescribers, upon request, provide any person designated to act on behalf of the patient with a copy of the patient's valid contact lens prescription, the Rule did not prescribe a time limit within which this copy had to be provided. The Commission proposed requiring that a prescriber respond to requests for an additional copy of a prescription within forty business hours. To facilitate patients' ability to use their prescriptions, another proposed change would require sellers to provide a mechanism that would allow patients to present their prescriptions directly to sellers.

Finally, the Commission proposed amending the prohibition on seller alteration of prescriptions to address concerns about the misuse of passive verification to substitute a different brand and manufacturer of lenses. The proposal requires a seller who makes an alteration to provide a verification request to the prescriber that includes the name of a manufacturer or brand other than that specified by the patient's prescriber. There is a proposed exception if the patient entered that manufacturer or brand on the seller's order form or the patient orally requested it from the seller.

The Commission will consider comments received in response to the SNPRM and, if appropriate, make changes before issuing a final rule.

2. **Chairman Simons, in the 114th Congress this Committee, on a party line vote with Republicans voting for and Democrats voting against, reported the Data Security and Breach Notification Act of 2015 to the House Floor. Under that bill, the FTC would currently have first offense civil penalty authority for data security incidents, including the Equifax breach.**

    a. **Do you still agree, as you did during our oversight hearing in 2018, that the FTC would benefit from having civil penalty authority for violations of the Safeguards Rule?**

Yes. Financial institutions subject to the GLB Safeguards Rule often maintain highly sensitive personal information of consumers. Financial institutions that are subject to the Safeguards Rule and that do not comply should be subject to civil penalties for first-time violations.

**3. Chairman Simons, when the FTC enjoyed broad rulemaking authority in the 1970s it got so bad that a Democratic-led Congress cut funding to the Commission for several days.**

**a. How should the events of the past inform our discussion about FTC rulemaking today and under future administrations**

Since the 1970s, Congress has enacted numerous laws that give the FTC discrete rulemaking authority in a variety of areas—children's privacy, privacy and data security for financial institutions, email marketing, telemarketing sales, and contact lens prescriptions, to name just a few. The FTC has exercised that rulemaking authority judiciously. In addition, rulemaking in all of these areas is subject to the procedural protections provided by the Administrative Procedure Act—including public notice and comment, a requirement that the Commission explain its reasoning, and an opportunity for judicial review. In its hearing testimony, the Commission requested similarly targeted APA rulemaking authority for consumer privacy and data security.

Since 1992, the FTC has also maintained a robust regulatory review program. All FTC rules and guides are reviewed periodically to ensure they are up to date, effective, and not overly burdensome. As part of the review process, the FTC solicits public input on issues such as the rule's economic impact; whether there is a continuing need for the rule; whether the rule may conflict with state, local, or other federal laws or regulations; and whether the rule has been affected by any technological, economic, or other industry changes. Decades of experience with targeted rulemaking and regulatory reviews have given the FTC a thorough understanding of rules' regulatory and economic impact, and will continue to inform the FTC's actions in the future.

**4. Chairman Simons, we know that small businesses have suffered in Europe since the implementation of the General Data Protection Regulation (GDPR). In fact, according to some reports, investments in startups are down an astounding 40 percent.**

**a. How can we guard against the same happening here?**

Because the GDPR has been in effect for only a year, there is a limited basis upon which researchers and others might draw conclusions about potential effects that the GDPR has had on investments in startups. That said, the FTC's recent *Hearings on Competition and Consumer Protection in the 21st Century* did include discussion of research showing that, in the European Union, the number of venture capital technology deals and the average amount invested per deal declined in the first several months after the GDPR took effect. Researchers have stated their intent to monitor to see whether those observations remain true on a longer-term basis, and whether they reflect correlation or causation. The FTC will keep abreast of such research.

**The Honorable Richard Hudson (R-NC)**

1. **In an article dated May 2, 2019, the Wall Street Journal reported that Facebook is interested in entering the payments and remittances markets as the company "aims to burrow more deeply into the lives of its users." The article also notes that one-third of the world's population logs on to Facebook on a monthly basis.**

    a. **Given Facebook's track record with consumer data, what concerns would FTC have if Facebook gained access to billions of people's sensitive financial data?**

The Commission has confirmed a non-public investigation into Facebook. It would be inappropriate to comment on potential practices of a company under investigation.

    b. **Given the potential scale of this business, what competition issues does FTC foresee? How will the FTC assure that other services will be able to compete against the likes of a Facebook?**

The Bureau of Competition recently announced the creation of a Technology Task Force ("TTF") that will enhance the Commission's antitrust focus on technology-related ecosystems, including technology platforms as well as markets for online advertising, social networking, mobile operating systems, and apps. The TTF will monitor competition in U.S. technology markets, investigate any conduct in these markets that may harm competition, and, when warranted, take actions to ensure that consumers benefit from free and fair competition.

2. **TechCrunch blog post entitled "Facebook is Pivoting" suggested that Facebook's recent moves indicate that it will evolve into a private end-to-end encryption platform for communication and commerce. The blog states that what "Facebook really wants next is for Messenger to become… an impregnable walled garden, used for business communications as well as personal, which dominates not just messaging but commerce." A situation "in which Instagram is the king of all social media, while Messenger/WhatsApp rule messaging, occupy the half-trillion dollar international-remittances space, and also take basis points from millions of daily transactions performed on" Facebook's platforms.**

    a. **As Facebook Inc. seeks to leverage its owned platforms to offer financial and other services, how is the FTC going to ensure Facebook responsibly manages this evolution into a financial and e-commerce giant?**

    b. **Given that Facebook touches one-third of the world's population and nearly two-thirds of all Americans, does the FTC have confidence Facebook will handle this evolution properly, given the company's history of handling sensitive data?**

The Commission has confirmed a non-public investigation into Facebook. It would be inappropriate to comment on potential practices of a company under investigation.