OFFICE OF
THE CHAIRMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

April 1, 2019

The Honorable Frank Pallone, Jr.
Chairman
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Dear Chairman Pallone:

Thank you for your March 20, 2019 letter requesting information about how the Commission would use additional resources to protect consumer privacy. The Commission has long exercised the authority Congress has given it under various statutes to address consumer privacy harms arising from new technologies and business practices. We have brought hundreds of privacy and data security cases, hosted about 70 workshops, and issued approximately 50 reports.

However, we need additional tools and resources to better protect consumers' privacy. I support federal privacy and data security legislation that would allow us to obtain civil penalties for violations, conduct rulemaking under the Administrative Procedure Act ("APA"), and exercise jurisdiction over common carriers and non-profits.

- First, as to civil penalties, the Commission can only obtain civil penalties against first-time violators for cases involving the Children's Online Privacy Protection Rule ("COPPA") or the Fair Credit Reporting Act ("FCRA"). To help ensure effective deterrence, we have urged Congress to enact legislation to allow us to seek civil penalties for data security and privacy violations in appropriate circumstances.
- Second, the ability to issue rules under the APA would enable us to better keep up with business and technological changes. Where we currently have APA rulemaking authority, we have used it judiciously. For example, in 2013, the FTC used its APA rulemaking authority to amend the COPPA Rule to address new business models, including social media and collection of geolocation information, that did not exist when the initial 2000 Rule was promulgated.
- Finally, any privacy and data security legislation should extend the FTC's jurisdiction to non-profits and common carriers, which often collect sensitive consumer information. Giving the FTC jurisdiction in these sectors would create a level playing field, ensuring that these entities would be subject to the same rules as others that collect similar types of data.

Regardless of any legislative changes, a significant increase in personnel would help the FTC ensure that American consumers' privacy is adequately protected. We currently have about 40 Full-Time Equivalents ("FTEs") devoted to privacy and data security issues—far fewer than

foreign data protection authorities. For example, the U.K. Information Commissioners' office has about 500 employees, and the Irish Data Protection Commissioner has about 110 employees. Although these entities have somewhat different mandates,[1] the contrast is stark. The FTC, as the federal entity primarily responsible for protecting consumers' privacy and data security in the United States (a much larger jurisdiction), should have more employees devoted to this effort.

You ask four specific questions about how the Commission would use additional resources, which I answer below.

1. **What resources would the FTC require to dramatically boost its enforcement activity with respect to privacy and data security? How would the FTC deploy new resources if it were to receive an additional $50 million for consumer protection and privacy? How about an additional $75 million? How about an additional $100 million? As part of your responses, please estimate the number of additional investigations and enforcement actions the FTC would likely be able to pursue.**

For the purposes of responding to this question, I assume that with $50 million in additional ongoing funding, we could hire approximately 160 more staff members; that with an additional $75 million annually, we could hire approximately 260 more staff; and that with an additional $100 million, we could hire approximately 360 more staff.[2] Assuming funding at these levels, I anticipate needing new management structures and support services to make the most effective use of these additional resources. Depending on the levels of additional funding and other considerations, below I have outlined one way in which we could allocate resources. We would, of course, consider any new privacy or data security legislation in determining how best to structure our work going forward.

Based on any of these three proposed levels of funding, we would consider adding at least three separate management units with the following responsibilities:

- **De novo enforcement:** One or more units would include some resources from our existing privacy division, which would be expanded to accomplish the following:
  - Devote additional staff to enforcement of the COPPA Rule;
  - Devote additional staff to financial privacy cases under the Gramm Leach Bliley ("GLB") Privacy and Safeguards Rules and the FCRA; and
  - Devote additional staff to Privacy Shield enforcement.

- **Order enforcement:** One or more units would include some resources from our existing enforcement division, and would expand the number of staff dedicated to conducting compliance reviews of our privacy and data security orders.

---

[1] For example, these entities enforce laws that protect consumers from government access to their data.

[2] Approximately two-thirds of our current budget is allocated to pay and benefits of staff, with about 16% allocated to overhead (such as rent and information technology) and the remaining 18% to other support expenses (such as expert witnesses, our consumer complaint database, and consumer and business education materials). Approximately 63% of our employees are attorneys or economists; the remainder are support staff such as investigators, technologists, and paralegals. In approximating the number of staff we could hire, we have assumed that any additional appropriation would be allocated similarly.

- **A new unit for policy, case generation, and targeting:** One or more units would be specifically devoted to conducting workshops, surveying legal developments in particular areas, writing advocacy comments and testimony, writing reports, and conducting 6(b) studies of industry. This unit would also include technologists to prepare original research on issues of interest, review referrals from privacy and security researchers, develop ideas for enforcement, and serve as a hub for technical expertise as needed on individual cases.

Each of these units would require new attorneys, paralegals, investigators, economists, administrative staff, electronic discovery staff, managers, and infrastructure (such as space). We would also plan to use some additional funds to pay outside experts in litigation and investigations, as privacy and data security investigations often involve complex facts and well-financed defendants.

You ask us to estimate the number of additional investigations and enforcement actions the FTC would likely be able to pursue. For reference, with our current allocation of about 40 staff devoted to privacy and security, we have brought on average about twenty privacy and data security cases per year over the past five years, and have investigated the privacy and security practices of many more companies. With more staff we would be able to bring more cases under our existing authority; providing us with additional authority would notably improve our ability to bring significantly more privacy and data security cases.

2. **If Congress were to direct the FTC to hire technologists to aid in case development, enforcement, rulemaking and/or policy recommendations, what resources would the FTC need to fulfill its consumer protection mission and how would the agency deploy those new resources? Specifically, describe the number of employees the agency would need, their roles and responsibilities, and how the FTC would use these resources to further its consumer protection mission.**

Currently, the Commission has about five full-time staff whose positions are classified as technologists. Beyond these specific full-time employees, the FTC has more than 40 investigators and lawyers who have developed technical expertise through their enforcement and policy work in the areas of big data, cybersecurity, the online advertising ecosystem, Internet of Things, artificial intelligence, and others. When the FTC needs more complex and richer information about a specific industry or technology, we supplement our internal technological proficiency by hiring outside technical experts to help us develop and litigate cases. We also keep abreast of technological developments in other ways, such as by hosting an annual event called PrivacyCon, in which we call on academics to present original research on privacy and security issues.

While we make the most of the technical resources we have, I believe we need to hire additional technologists to provide better support for our current enforcement and policy work. These technologists would serve the following roles:

- **Conducting original research:** Our existing Office of Technology Research and Investigation has conducted original research into, for example, data collection by children's apps, and the use of email authentication and anti-phishing technologies by

web-hosting services that market themselves to small businesses. With additional technologists, we would be able to conduct more studies of this nature.

- **Assisting in case targeting and development:** We currently have only around three technologist FTEs available to keep abreast of privacy and security research, work with attorneys to determine appropriate matters for investigation and enforcement, and to develop investigational plans to determine what evidence we might need to support a technology-related case. We could use more technologists to serve this function.
- **Serving on case teams:** The same three technologist FTEs noted above also review technical documents that we obtain in investigations and litigation; help attorneys conduct interviews, investigational hearings, and depositions of technical staff at companies; and provide technical advice to lawyers. Additional technologists would deepen and strengthen our litigation capabilities.
- **Pursuing technical tools for agency use in investigations:** Additional technologists could assist the Commission with acquiring or developing internal technical tools to analyze products and services for potential law violations.
- **Assisting with policy projects**: We could use additional technical expertise to support various technical policy projects. For example, last year we announced the results of our "IoT Home Inspector Challenge," in which we awarded prize money for a contest to create a way for consumers to be able to more easily update and patch Internet of Things' devices in their homes. A technologist assisted with that project, and additional technologists could assist with similar projects in the future. We could also use additional technologists to assist in drafting 6(b) orders for industry participants, and analyzing responses to those orders, to help us better understand specific industries and business practices.

To fulfil these roles, we anticipate needing 10-15 additional technologists. If the Commission were to receive significant new appropriations to boost its privacy and data security enforcement work, we would need to invest in even more technologists. Because current civil service rules for hiring can be time-consuming and inflexible in ways that might hinder our ability to attract and hire candidates with the most current and relevant experience, we are exploring how to classify these positions such that we could use direct authority for hiring.

3. **If the FTC received notice-and-comment rulemaking authority with respect to privacy and data security, would the FTC require additional resources to develop and update new rules without detracting from the agency's enforcement activity? If so, what resources would the FTC require?**

Yes. When Congress passed the Fair and Accurate Credit Transactions Act ("FACTA"), which amended the FCRA and resulted in the Commission creating more than ten separate Rules, the Commission spent more than 50,000 staff hours over the next three years on its implementation. This equates to eight full-time employees dedicated solely to that project for three years. We estimate that engaging in notice-and-comment rulemaking for comprehensive privacy or data security legislation would require at least the same, if not more, staff hours.

4. **What would the FTC be able to accomplish with 100 new attorneys focused on privacy and data security that it cannot do with current resources?**

The appropriation by Congress of money to bring in – and, importantly, continue to pay for – 100 new attorneys focused on privacy and data security would have a significant impact on the work of the Commission. With these additional resources, the FTC could devote more time not only to case generation and enforcement, but also to keeping abreast of new technologies and areas of privacy and data security concern through workshops, reports, and industry studies. The Commission would also be able to devote additional resources to compliance monitoring of companies under order for privacy and data security failures, and to engage in additional order enforcement litigation. Importantly, as described above, any influx of additional attorneys would also require additional appropriations for infrastructure, outside experts, and support staff such as technologists, paralegals, and investigators.

We appreciate your support of the Commission's efforts in the privacy and data security area. Should you need any additional information, please contact Jeanne Bumpus, Director of the FTC's Office of Congressional Relations, at (202) 326-2946.

Sincerely,

Joseph Simons
Chairman