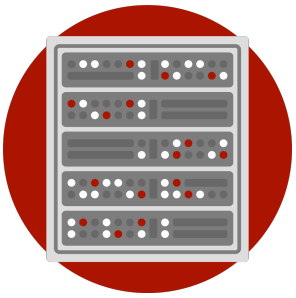
Federal Trade Commission
1700 Pennsylvania Avenue, NW
Washington, DC
Submission via online portal

INTERNET INFRASTRUCTURE COALITION



i2Coalition.com

718 7th Street NW
2nd Floor
Washington DC 20001

contact@i2coalition.com

(202) 524-3183

RE: i2Coalition Response to Docket ID: FTC-2018-0052, The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters

The Internet Infrastructure Coalition (i2C) appreciates the opportunity to provide comments on the Federal Trade Commission's (FTC) concerns with respect to privacy and data security. Our coalition is made of up mainly small to medium sized businesses and is comprised of cloud providers, data centers, registrars, registries and other foundational Internet enterprises. The organization was founded by a group of companies initially involved in advocacy for a free and open Internet. Those values remain as our guiding principles. It is with these principles in mind that we offer our concerns and suggestions about the FTC's remedial authorities.

Any New FTC Regulatory or Enforcement Activity Should Be Scalable and Contemplative of Industry Diversity

Given the makeup of our membership, we support privacy and data security protections but have ongoing concerns about the scalability of agency actions. Business sizes and actual capacity to respond to enforcement should be taken into account when drafting new rules. For some enterprises, the costs of responding to a lawsuit or administrative actions that are overly broad or highly restrictive in the requirements for response times could mean the end of businesses. For others, takedowns or cease and desist orders can be difficult because of staffing issues or because of competing requests from administrative agencies and law enforcement.

When broadly defining rules and legislation to the "Internet industry" or "digital economy", there is a risk of impacting businesses which do not handle certain kinds of data or do not store data. For example, domain name registry operators (wholesalers) typically do not have direct contact with the individuals or organizations purchasing second-level domain names from registrars (retailers). As such, a domain name registry would have no direct relationship with the individual or entity engaged in unfair or deceptive conduct and would have no further contact with the uses or handling of said data. This is similarly true with registrars and data centers which provide a certain kind of real estate or access but do not directly manage what clients do with the product. We ask that the agency consider the diversity of industry actors and their respective lines of business when defining the scope of its jurisdiction and writing new policies with respect to enforcement activities. Any new policies should scale both up and down, taking into account the fact that those businesses focused primarily on the Internet are not unitary. Using the domain name registry example above, an FTC policy that requires contacting a customer following a data breach would permit the retail registrar to contact the customer using the information provided by the customer at the time of registration but recognizes that the wholesaler registry operator typically does not have a direct relationship with the domain name owner (registrant). This type of policy creates consumer confidence in the

security of the business, while at the same time acknowledging that the business may not have continuous contact with its customers.

Section 5 Enforcement Should Be Harm or Evidence-Based

There are some that believe the FTC has limited jurisdiction under Section 5 however the text is quite broad ("unfair methods....unfair acts or deceptive practices affecting Commerce") and gives the agency a fair amount of latitude in its enforcement work. In its own review of its 2017 enforcement efforts, the FTC stated that it brought more than 180 enforcement cases that year. That includes 130 spam and spyware cases and 50 general privacy actions. The common thread in each of these cases typically is that the agency actions were based on actual harm to consumers, as in the SQ Capital and Stark Law cases, or they were evidence-based or shown to have relevant proximity to actual harm to individual consumers.

Juxtapose this situation with the 11th Circuit outcome in the LabMD case in which the court upheld an administrative decision based on the finding that the FTC's position was not based on a specific action that would fall under the auspices of Section 5. Rather, the agency position was based on activities the actor ought to or should have done. When the approach is harm or evidence-based, the agency has more certainty of being within its Section 5 powers and thus more successful in its enforcement efforts. Businesses looking to a consistent application of those agency powers can also find certainty about their scopes of conduct and legal responsibilities. This type of certainty is particularly important for the small to medium-sized business that makes up the bulk of Internet businesses.

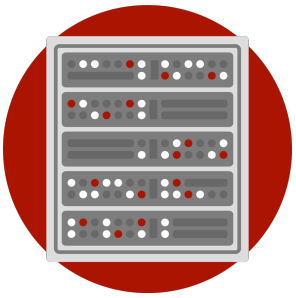
Need for Coordination With Inter-Agency and Private Industry

In addition to the rights and procedural requirements contemplated in the 1st, 9th, and 14th Amendments, the Agency has a lens into privacy protections based on a number statutes including, but not limited to: HIPPA, The Privacy Act of 1974, The Financial Monetization Act, the Fair Credit Reporting Act, The Children's Online Privacy Protection Act, its own Section 5 powers; and a number of rules including, but not limited to: the Red Flags Rule, the CAN-SPAM Rule, and the Prescreen Opt-out Rule. Within each of these the FTC has jurisdiction, but on some level shares investigative and/or enforcement powers with other agencies such as the SEC and law enforcement. Before issuing new rules or advocating for new legislation, it would be helpful for the agency to have a comprehensive review of 1) what is an appropriate expression of existing powers in the digital economy, 2) the applicability of those powers and 3) whether the agency is engaging with its inter-agency partners to ensure enforcement is efficient and effective both from the consumer and private industry standpoints.

Need for more advocacy and education

In the past, the FTC has done robust work in advocacy to other parts of government such as the NTIA and Office of Science and Technology Policy. Two illustrative examples are the Agency's work on the restoration of jurisdiction over broadband services to the FCC and its guidance on Internet of Things (IoT) device manufacturers on security vulnerabilities. In the former, that change in jurisdiction would naturally expand the agency's existing enforcement powers.

INTERNET INFRASTRUCTURE COALITION



i2Coalition.com

718 7th Street NW
2nd Floor
Washington DC 20001

contact@i2coalition.com

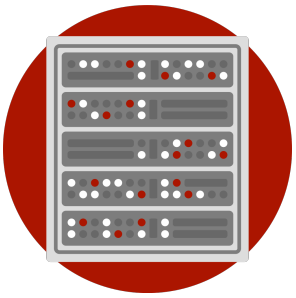
(202) 524-3183

In its advocacy work, the FTC has engaged in consumer education on other topics such as IoT devices and protection of children online. In this context, further work on managing data and good personal security practices would be a helpful complement to any policy updates. This aspect of the FTC's work is clearly illustrated in FTC arguments in the LabMD case. These arguments made very good educational and best practices suggestions for small and medium-sized business, such as requiring employees with remote access to use VPN or other secure authentication protocols.

In addition to its existing advocacy efforts, a concept the FTC could explore is a workshop or symposium on data security. It could include best practices information and mitigation tools for both consumers and businesses. In addition to, or as part of its annual review, the FTC could also include an annual security review. This could be something akin to a "State of Security" report or a trend and threat analysis. It would be an opportunity to engage industry experts and consumers.

Finally, we support efforts to protect consumers and our larger economy from bad actor and inappropriate state or private industry actions. We would like to see enforcement powers scoped and for the agency to consider the diversity of the industries within its jurisdiction when making enforcement decisions. The coalition also looks forward to being a resource to the Federal Trade Commission and assisting with any advocacy or education efforts.

INTERNET INFRASTRUCTURE COALITION



i2Coalition.com

718 7th Street NW
2nd Floor
Washington DC 20001

contact@i2coalition.com

(202) 524-3183