HackerOne
300 Montgomery Street 12th Floor
San Francisco, CA. 94104

November 8, 2018

Re: Docket No. 180821780-8780-01

National Telecommunications and Information Administration ("NTIA")
U.S. Department of Commerce
1401 Constitution Avenue. NW, Room 4725
Attn: Privacy RFC
Washington, D.C. 20230
Sent via email to privacyrfc@ntia.doc.gov

To whom it may concern:

Thank you for the opportunity to comment on the Department of Commerce's ("Commerce Department") Approach to Consumer Privacy. As HackerOne's mission is to provide a safer internet for all, we applaud the efforts of the Commerce Department and NTIA to protect consumer privacy. Because consumers are increasingly reliant on digital services and those services involve a complicated web of technology, consumers must understand what is happening with their personal information. Therefore, we strongly agree with the Commerce Department's statement that consumer trust should be at the core of the United States policy formation. Consumers must understand what information is being collected, what it's being used for, and how it's being protected.

As the Commerce Department recognizes, protecting consumer data is hard, and burdensome regulations do not necessarily result in increased privacy protections. Therefore, we endorse the Commerce Department's outcome-based approach that focuses on flexibility and the minimization of risk. HackerOne believes that the best outcome, in order to ensure the trust of consumers, is the reduced risk of a data breach. Because HackerOne is an expert in the area of coordinated vulnerability disclosure and represents the interests of hundreds of thousands of ethical hackers, we actively encourage businesses to work with them.

We respectfully submit comments to Section I (A) (4) and Section (I) (B) (7).

Section I (A) (4) "Security". We recommend additional clarity to the following sentence:

"…organizations should take reasonable security measures appropriate to the level of risk associated with the improper loss of, or improper access to the collected personal data; they should meet or ideally exceed current consensus best practices, where available."

We recommend references to some of those best practices in security. One of the best security practices is coordinated vulnerability disclosure.

The NTIA has taken the lead on coordinated vulnerability disclosure. As stated in the Early Stage Coordinated Vulnerability Disclosure Template, Version 1.1, on page 2, when discussing "safety-critical industries," the NTIA Working Group recognized that "Coordinated vulnerability disclosure directs energy and attention into improving the safety and security of systems and software for the overall population."

In addition to the NTIA's thoughtful work, coordinated vulnerability disclosure is fast becoming accepted as a best practice across all types of industries, and recommended by federal and international standards bodies. Here is a notable list:

- "Coordinated disclosure may no longer be considered just one of many possible facets of an organization's cybersecurity program, but an indispensable cornerstone." Energy and Commerce Committee Majority Staff: The Criticality of Coordinated Disclosure in Modern Cybersecurity, October 23, 2018. https://energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf
- Department of Justice (DoJ) published a Framework for a Vulnerability Disclosure Program for Online Systems. https://www.justice.gov/criminal-ccips/page/file/983996/download
- The Food and Drug Administration ("FDA") issued the "Postmarket Management of Cybersecurity in Medical Devices" to inform industry and FDA staff of the Agency's recommendations for proactively managing cybersecurity vulnerabilities, and it plans to consider new postmarket authority to require that firms adopt policies and procedures for coordinated disclosure of vulnerabilities as they are identified. https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf (page 14)
- ISO 29147: recommends vulnerability disclosure as a best practice and offers guidelines on how to include in their processes when receiving information about potential vulnerabilities from external individuals or organizations.
- NIST Cybersecurity Framework: Provisionally added RS.AN-5 which recommends that processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

We suggest not waiting for enforcement actions to determine what "reasonable" means in the context of privacy as it relates to best security practices. Instead, HackerOne believes that the Department of Commerce should expressly state that coordinated vulnerability disclosure is a best practice because it achieves the desired outcome of reducing the risk of data breach.

Section 1 (B) (7) "FTC enforcement". We fully support ensuring the FTC has the necessary resources, clear authority and direction to enforce consumer privacy laws. When discussing two cases, the FTC recommends a vulnerability disclosure policy:

- "The lesson for other businesses? Have an effective process in place to receive and address security vulnerability reports. Consider a clearly publicized and effective channel (for example, a dedicated email address like security@yourcompany.com) for receiving reports and flagging them for your security staff." https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (page 12).

Finally, we note that the RFC does not include when consumers should be notified of data compromises for nefarious uses. We suggest that a provision be added to state that this type of compromise should be viewed as material, and a consumer should be promptly notified. Further, because the Securities and Exchange Commission is very interested in cybersecurity, we also suggest coordinating with them to issue further guidelines as to what would be considered a material data breach.

In closing, we are extremely pleased that the Department of Commerce is taking an active stance in the area of privacy. Thank you again for the opportunity to comment.

/s/ Deborah Chang

Deborah Chang
VP Business Development and Policy
HackerOne