Comments of the American Consumer Institute on the "Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201", U.S. Federal Trade Commission. Docket ID No. [FTC-2018-0048] August 13, 2018

Thank you for the opportunity to submit comments regarding the "Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201." These comments are being submitted on behalf of the American Consumer Institute Center for Citizen Research (ACI).

ACI is a nonprofit 501(c)(3) educational and research institute with the mission to identify, analyze and project the interests of consumers in selected legislative and rulemaking proceedings in information technology, health care, insurance, energy and other matters. Recognizing that consumers' interests can be variously defined and measured, and that numerous parties purport to speak on behalf of consumers, the goal of ACI is to bring to bear the tools of economic and consumer welfare analyses as rigorous as available data will allow, while taking care to assure that the analyses reflect relevant and significant costs and benefits of alternative courses of government action.

The main focus of this submission is the Federal Trade Commission's (FTC) current and future role in protecting consumer privacy and security and ensuring the competitiveness of U.S. markets while not imposing unnecessary costs on private parties or governmental processes.

We commend FTC's policy efforts to keep pace with changes in the economy by staying committed to self-examination and critical thinking towards its policy of continuity. As the FTC thinks about re-evaluating its approach on current and anticipated competition and consumer protection issues, it should be mindful of the following potential challenges associated with changes in the economy, evolving business practices, and new technologies:

Security goals and privacy requirements can sometimes clash.[1] The ability to evaluate and fix cybersecurity vulnerabilities will heavily depend on parties sharing information, and government-mandated security requirements aim to limit encryption technologies on the reasoning that the growing use of encryption could seriously hinder criminal and national security investigations. Yet, the prospect of intentionally weakening encryption techniques can be dangerously problematic as they could create back doors for cyber-attacks.[2]

Since security issues are not intrinsically static, prescriptive cybersecurity regulations are less flexible and less likely to be responsive to changing contexts and circumstances. For example, cybersecurity regulations mandated in 2018 could likely be outdated and possibly

[1] Ellen Nakashima and Barton Gellman, "As encryption spreads, U.S. grapples with clash between privacy, security," *The Washington Post*, April 10, 2015, https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html?utm_term=.579fa48e69ae.

[2] Andrea O'Sullivan, "Giving Government 'Backdoor' Access to Encrypted Data Threatens Personal Privacy and National Security," *Reason*, June 16, 2015, https://reason.com/archives/2015/06/16/crypto-wars-weaken-encryption-security.

completely obsolete by 2020. FTC should avoid establishing a rigid regulatory framework, which will interfere with developing private industry standards and crowd out investment, innovation, market experimentation, new business models and competition. Instead, the FTC should seek to provide guidance and facilitate the development of industry-established best practices. There are already numerous industry-established security standards that set a very high bar (e.g., automotive and wireless services industries).[3] The FTC should continue collaborating with the industry to develop new guidance and updated best practices based on new technologies.

Top-down privacy and security policy prescriptions often tend to backfire, creating technology bottlenecks and reducing consumer welfare.[4] The FTC should avoid one-size-fits-all policy mandates and focus on encouraging collaborative, multi-stakeholder initiatives and approaches to improve security and privacy.

FTC should be especially cautious of over-regulating infant and emerging industries and new technologies. The danger here being, overregulation or poorly-designed regulation, would retard the growth of infant industries and slowdown the development of private industry standards.

FTC should make sure that a strategy for security and privacy does not come at the expense of improved products and services, which could undermine consumer welfare by diminishing competition, producing fewer choices, increasing industry costs and consumer prices, and repressing consumer demand. FTC should prioritize conducting thorough benefit-cost analyses of any proposed regulations. At a minimum, the analyses will enable FTC to determine whether the projected consumer welfare from proposed regulations outweigh the likely costs associated with compliance, implementation and enforcement of new rules.[5]

FTC should continue to educate the public about privacy and security risks, especially those risks associated with new technologies.[6] Because imperfect information can be a market failure, it is imperative that consumers be given the information necessary to make good market decisions surrounding the use of their information, privacy and security.

---

[3] For industry examples, see Automotive Information Sharing and Analysis Center, August 2018, https://www.automotiveisac.com/index.php; and "Messaging Principles and Best Practices," CTIA, January 19, 2017, https://api.ctia.org/docs/default-source/default-document-library/170119-ctia-messaging-principles-and-best-practices.pdf.

[4] Thierer, Adam, *"Permissionless Innovation: The continuing case for comprehensive technological freedom,"* Mercatus Center, George Mason University, 2016, at https://www.mercatus.org/publication/permissionless-innovation-continuing-case-comprehensive-technological-freedom.

[5] Thierer, Adam. "A Framework for Benefit-Cost Analysis in Digital Privacy Debates, " George Mason Law Review 20: 1055, 2012, at https://www.mercatus.org/publication/framework-benefit-cost-analysis-digital-privacy-debates.

[6] The FTC already provides (in partnership with other federal agencies) OnGuardOnline, a website that offers wide-ranging security, safety, and privacy tips for both consumers and businesses. See https://www.onguardonline.gov/.

> Empowering consumers through education should be preferable to prescriptive regulation.[7] This approach can provide more flexibility than administrative regulations, particularly in the case of online policy issues.[8]

In summary, given current and on-going changes in the economy, evolving business practices, new technologies and international developments, the American Consumer Institute urges the FTC to give the recommendations (outlined above) serious reflection in its approach to these competition and consumer protection issues.

Thank you for your time and consideration of these comments.

Sincerely,

Krisztina Pusok
Director of Policy and Research
American Consumer Institute
Center for Citizen Research
1701 Pennsylvania Avenue, NW
Suite 200 Washington, DC 20006

[7] Thierer, Adam. "A Framework for Benefit-Cost Analysis in Digital Privacy Debates. "
[8] Ibid.