

Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of)
)
Competition and Consumer Protection in)
The 21st Century: The Role of Intellectual)
Property and Competition Policy in)
Promoting Innovation)

COMMENTS OF NEW AMERICA’S OPEN TECHNOLOGY INSTITUTE

August 20, 2018

Andi Wilson Thompson
Ross Schulman
New America’s Open Technology Institute
740 15th St NW Suite 900
Washington, D.C. 20005

Introduction

New America's Open Technology Institute (OTI) respectfully submits these comments in response to the FTC's request for comments in advance of the upcoming hearings on Competition and Consumer Protection in the 21st Century. Our comments will specifically focus on Question 5, regarding the FTC's remedial authority to deter unfair and deceptive conduct in privacy and data security matters, and the potential for additional tools to assist in this process.

The remedial authority of the FTC to hold companies accountable for privacy violations or data breaches is extremely important in encouraging companies to take steps to protect the security and privacy of their users. FTC investigations, threats of fines being levied against them, or other penalties are important tools to force companies to protect consumers. However, these processes and authorities do not necessarily stop the products from getting into the hands of users. Consumers, specifically, are not the audience for FTC enforcement mechanisms.

The Digital Standard can help fill that gap.¹ As a consumer-focused digital security project, its goal is to educate people about the privacy and security aspects of the internet-connected devices they are thinking of purchasing. If it is successful, the Digital Standard will work to place market pressure on manufacturers to implement better consumer protection practices by way of educating consumers, complementing the FTC's enforcement authority.

What is the Digital Standard?

The Digital Standard is an open, collaborative effort to create a digital privacy and security standard which can help guide the future development of consumer software, digital platforms and services, and internet-connected products.² The Standard methodology is composed of 35 different "tests" that products can be measured against to see how well they meet industry best practices. It also provides a model that companies can use to design and improve their products, ensuring that they are the best in class on these security and privacy metrics.

The Digital Standard was developed as a collaboration between civil society groups Disconnect,³ Ranking Digital Rights,⁴ the Cyber Independent Testing Lab,⁵ and Aspiration,⁶ as well as ratings organization Consumer Reports.⁷ This open-source process included contributions from cybersecurity experts who evaluated the tests and methodology from a technical perspective. This process gives it legitimacy as a framework that was developed with the interests of consumers, rather than companies, in mind.

¹ "Raising The Standard," New America's Open Technology Institute, <https://www.newamerica.org/oti/raising-standard/>.

² "The Digital Standard," available at <https://www.thedigitalstandard.org/>.

³ "Disconnect: Who We Are," <https://disconnect.me/about>.

⁴ "Ranking Digital Rights," <https://rankingdigitalrights.org/>.

⁵ "Cyber ITL," <https://cyber-itl.org/>.

⁶ "Aspiration," <https://aspirationtech.org/>.

⁷ "Consumer Reports," <https://www.consumerreports.org/cro/index.htm>.

Manufacturers and developers may also have an economic interest in conforming to the Digital Standard because of the influence rating organizations can have on their customers. In fact, Consumer Reports is planning to incorporate digital security and privacy metrics into its existing ratings process. It has already used the Standard to rate Smart TVs⁸ and payment applications.⁹ When products that were previously tested for screen resolution and sound clarity suddenly receive poor reviews because of security vulnerabilities, companies could have an incentive to adhere to best practices. When a ratings process has the ability to both give positive as well as negative reviews, it has more potential to move the market.

This leads to a more effective outcome than with a standard like Energy Star – a self-certification metric which grades energy efficiency but fails to clearly highlight inefficient products.¹⁰ In this case, a framework like the Digital Standard could provide a tool to assist in the development of new products, allowing inexperienced companies to build new models with security features baked in. Companies without much experience in digital security, such as pre-digital appliance or household tools manufacturers who have only recently added connected capabilities to their products, may not have the skills or knowledge to implement the necessary protections for security and privacy. The Standard is also still under development, with opportunities for stakeholders to contribute feedback and expertise into the testing metrics and process.

Next Steps

In order to benefit from the Digital Standard’s potential as a supplemental tool for encouraging companies to adhere to better privacy and security best practices, the FTC should do three things. First, learn more about the Standard, discussing the process with experts, and investigating potential ways that it can be used to compliment FTC work on digital security best practices. Second, finding ways that the FTC could speak publicly in support of processes like the Standard would be extremely valuable in incentivising companies to look toward implementation of this set of best practices. Third, the Standard is still under development, with opportunities for stakeholders to contribute feedback and expertise into the testing metrics and process. Further engagement from stakeholders can create a more robust evaluation and development tool, and establish the Digital Standard as the best practice for IoT device security. Any feedback that the FTC could provide to help further refine the process would provide important perspective from such an influential agency.

Conclusion

OTI appreciates the opportunity to submit comments in advance of the upcoming hearings. Given the the rapid expansion of the IoT market, and how many companies are entering the

⁸ “Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds,” Consumer Reports, February 7, 2018, <https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/>.

⁹ “Peer-to-Peer Payments Are Generally Safe, But Consumers Must Be Aware of Risks,” Consumer Reports, August 6, 2018, <https://www.consumerreports.org/digital-payments/peer-to-peer-payments-are-generally-safe-but-consumers-must-be-aware-of-risks/>.

¹⁰ ENERGY STAR Overview,” <https://www.energystar.gov/about>.

connected devices space, a tool like the Digital Standard is key to ensuring that these devices adequately protect the security and privacy of consumers.