Additional Questions for the Record
Subcommittee on Consumer Protection and Commerce
Hearing on
"Transforming the FTC: Legislation to Modernize Consumer Protection"
July 28, 2021

Graham Dufault, Senior Director for Public Policy, ACT | The App Association

The Honorable Janice D. Schakowsky (D-IL)

1. The central theme of last month's hearing was ensuring the FTC has the tools it needs to protect consumers in the modern marketplace and into the future. In practice, this often means adapting to an online, interconnected world.

    a. How has the shift to online commerce, the proliferation of social media, and the general dependence on the internet changed the consumer experience?

    RESPONSE:

Online Commerce. For App Association members, one of the most significant developments that shifted commerce into the online space was the introduction of the smartphone and the entry of the software platform distribution model to the marketplace. In the early and mid-2000s, independent companies that sold software faced uphill battles to reach their addressable markets.[1] For consumers, downloading software from an unfamiliar developer was a gamble: often, bad actors took advantage of the availability of software on the open internet, posing as legitimate companies to plant malware on personal computers (PCs). The smartphone and software platforms (app stores bundled with mobile operating systems) changed this dynamic in ways that have undeniably benefited small software companies and consumers alike.

First, the entry of software platforms brought with it a greater variety of choices, lower prices, and higher quality products and services for consumers.[2] From the time they first carried software made by independent companies like App Association members, the major app stores performed vetting functions, approving and denying third-party apps.

[1] *See* ACT | The App Association, The Symbiotic Relationship Between App Developers and Platforms: A Ten-Year Retrospective (2018), *available at* https://actonline.org/wp-content/uploads/2018_ACT-App-Store-Ten-Year-Retro-Doc.pdf.

[2] *See* Hearing on "Competition in Digital Technology Markets: Examining Self-Preferencing by Digital Platforms," before the United States Senate Judiciary Committee Subcommittee on Antitrust, Competition Policy, and Consumer Rights (116th Cong., 2d Sess.), statement of Morgan Reed, president, ACT | The App Association (Mar. 10, 2020), *available at* https://actonline.org/wp-content/uploads/2020-03-07-ACT-Testimony-Senate-Judic-Antitrust-Sub-Hrng-FINAL.pdf.

The process they use has improved over the years[3] and complements the operating system features software platforms employ to prevent access to consumer data and device features by bad actors. Together, these platform functions created and maintain a trusted marketplace for consumers to conduct online commerce in all of its various and evolving forms. Second, software platforms provide a bundle of developer services that include worldwide distribution, developer tools, assistance with intellectual property protections, and most importantly, the ability to leverage a trusted marketplace to sell software and other products and services ancillary to an app.[4] Before software platforms developed this bundle of services, independent software companies cobbled them together at higher costs to reach their intended markets. The cultivation of trust in the software company's brand alone often took years to establish. These overhead costs combined with generally smaller addressable consumer and business markets, resulting in less attractive prospects for developers and far fewer choices and higher costs for consumers and clients. A key litmus test for our member companies is whether consumers are willing to download software from a company they had never heard of previously. Under current circumstances on software platforms, consumers are able to download such software confidently because they know platforms actively bar and remove apps with malware and other harmful content. Many App Association members sell products and services on the open internet as well and it can be a substitute for software platform distribution. But without software platforms, far fewer app makers would be able to scale up quickly enough and become competitive, and consumer choice would suffer as a result.

The Federal Trade Commission (FTC) has rightfully focused on potential consumer harms accruing from intentional bad actors or from otherwise unintentional unfair or deceptive practices on the app stores. Software platforms play a key role in managing an app ecosystem that offers consumers a wide variety of options, while minimizing financial, safety, and privacy risks. These management functions form the core of the bundle of developer services described above, without which consumer trust would begin to collapse. Some proposals in Congress, like the Open App Markets Act (H.R. 5017 / S. 2710) and the American Choice and Innovation Online Act (H.R. 3816) would prohibit these management functions, ostensibly to address complaints from competitors with alternative products and services on the platform. While the bills would benefit some large competitors like Epic Games and Spotify, they would harm small app makers like App Association members as well as consumers because they would erode the trust consumers have in being able to conduct digital commerce in the app marketplaces. Both H.R. 5017 and H.R. 3816 would create a presumption that important software platform privacy and security features are illegal. The bills essentially allow platforms to overcome that presumption only by showing that any measure they take was "narrowly tailored,

---

[3] Anna Bosch, "A Brief History of Time: The App Stores," ACT | The App Association Blog (Apr. 7, 2021) *available at* https://actonline.org/2021/04/07/a-brief-history-of-time-the-app-stores/.
[44] *See* ACT | THE APP ASSOCIATION, THE SYMBIOTIC RELATIONSHIP BETWEEN APP DEVELOPERS AND PLATFORMS: A TEN-YEAR RETROSPECTIVE 3 (2018), *available at* https://actonline.org/wp-content/uploads/2018_ACT-App-Store-Ten-Year-Retro-Doc.pdf.

could not be achieved through a less discriminatory means, was nonpretextual, and was necessary"[5] to provide privacy. The House Energy and Commerce Committee should oppose measures like these as moving federal policy in the opposite direction from where it should be heading. Congress should not *prohibit* privacy controls that are proven to work; instead, it should *require* companies to adopt privacy protections. Otherwise, federal law would undo the privacy-protective developments that enable online commerce, forcing consumers to accept a single, more open approach to security, or even worse, back to an early 2000s online experience with fewer options, less meaningful privacy protections, and diminished security.

Proliferation of social media. App maker interests largely center on software, rather than social media, platforms. However, to the extent that social media platforms have introduced and rapidly expanded the use of large data sets about their users, app makers have equities at stake. Many of our member companies rely on the ability to conduct analytics that draw on individuals' online activities, including how they use the software products and services that our member companies design. They also place ads using ad networks that target ads to certain kinds of consumers or in certain contexts in order to acquire new customers and clients. However, the tendency for the ad-driven "free to the consumer" model to lead to uses of data to which a consumer never consented, or that otherwise push the boundaries of activities conducted under color of authorization, has harmed App Association members. In some instances, small app companies used software development kits (SDKs) from large social media platforms that suggest they are not collecting data but turn out to be doing just that, in order to feed ad networks. While an inflexible notice-and-consent privacy regime is not a workable solution, companies should use data only in ways that comport with the consumer's reasonable expectations given the context of their relationship with the company. The House Energy and Commerce Committee's staff draft privacy legislation includes a provision that is consistent with this approach, providing that affirmative consent is not required and consent implied "to the extent the processing is consistent with the reasonable consumer expectations within the context of the interaction between the covered entity and the individual . . .."[6] The consumer experience with social media platforms underscores why a strong privacy law should bar processing and collection activities that are inconsistent with consumer expectations. Allowing this activity to go unchecked directly erodes the trust consumers have in the app ecosystem and in online services generally, which is central to the survival and success of App Association members.

General dependence on the internet. In the past year, digital transactions increased 42 percent and 60 percent of those transactions were mobile.[7] Our increased reliance on online products and services permeates virtually all aspects of our daily lives, from how we

[5] American Choice and Innovation Online Act, Sec. 2(c)(1)(B) (H.R. 3816, 117th).
[6] House Energy and Commerce Committee staff draft privacy legislation, ___ Act of 2019, Sec. 6(b)(1) (H.R. ___, 116th).
[7] LEXISNEXIS RISK SOLUTIONS, FRAUD TRENDS TO WATCH IN 2021 (2021), *available at* https://risk.lexisnexis.com/insights-resources/infographic/fraud-trends-to-watch-in-2021.

get lunch to how we access healthcare. Privacy and security risks attend any online service, interaction, or transaction. Bad actors are redoubling their attacks on smart devices in particular, as mobile device fraud attacks increased by 48 percent.[8] More demand for App Association member products and services has benefitted the app economy, but it also increases the need for better cybersecurity awareness and tools. Our member companies must be able to employ strong technical protection measures like encryption and benefit from and participate in real-time cybersecurity threat sharing. Similarly, our inevitable reliance on online services underscores again the importance of allowing software platforms to cultivate a dependable marketplace and of Congress' important role in imposing a single set of strong, federal privacy requirements to improve protections and trust in the online marketplace.

b. Are certain groups particularly vulnerable to online harms?

RESPONSE:

Small businesses are especially vulnerable to cyberattacks, as 60 percent of small companies go out of business within six months of a breach.[9] As I described in testimony before the House Small Business Committee, small businesses are not as well equipped as they should be to thwart these attacks.[10] A single set of requirements at the federal level for data security would help prevent the devastating effects of these attacks by making small businesses less attractive targets and less vulnerable to scams. Similarly, this Committee is right to explore options to better position federal enforcers to investigate cybercrime and punish perpetrators. The Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies (RANSOMWARE) Act (H.R. 4551) would also help policymakers sharpen enforcement against ransomware attackers overseas.

As far as certain demographics that are especially vulnerable to online harms, statistics suggest that consumers under 25 and over 75 are also more vulnerable to online harms, especially those that result from bad actors through social engineering.[11] The FTC's own data points to fewer reports of dollar losses by older consumers but higher median losses per attack.[12] The evidence here supports action by the Committee to direct the FTC's

---

[8] *Id.*
[9] PURPLESEC, CYBER SECURITY TRENDS IN 2021 (Apr. 29, 2021), *available at* https://purplesec.us/resources/cyber-security-statistics/.
[10] Hearing on "Strengthening the Cybersecurity Posture of America's Small Business Community," before the House Small Business Committee (117th Cong., 1st Sess.), statement of Graham Dufault, Senior Dir. for Pub. Policy, ACT | The App Association (Jul. 20, 2021), *available at* https://smallbusiness.house.gov/uploadedfiles/07-20-21_mr._dufault_testimony.pdf.
[11] "Cybercrime report finds young adults and adults over 75 most vulnerable to fraud attacks," SECURITY MAGAZINE (Feb. 25, 2021), *available at* https://www.securitymagazine.com/articles/94684-cybercrime-report-finds-young-adults-and-adults-over-75-most-vulnerable-to-fraud-attacks.
[12] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 2020 13 (Feb. 2021), *available at* https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf.

focus on elder fraud and the FTC Robust Elderly Protections and Organizational Requirements to Track Scams (FTC REPORTS) Act (H.R. 2672) would help in this regard. Similarly, recent FTC data also indicates that members of the military community reported higher median losses due to fraud than the public at large.[13] Therefore, the Veterans and Servicemember Consumer Protection Act of 2021 (H.R. 4483) is also a welcome measure to ensure the FTC focuses its enforcement efforts on fraud schemes tailored to the military community. Lastly, as fellow witness Sally Greenberg of National Consumers League pointed out, "affinity fraud" threatens a variety of demographics, as fraudsters are known to target consumers based on their sexual identity, ethnicity, religion, race, and other protected characteristics.[14] The Consumer Equity Protection Act (H.R. 4460) is therefore a welcome measure to help direct the FTC's efforts to combat fraud schemes specifically targeting these communities.

Since fraudsters are ramping up their attacks on vulnerable populations and businesses in the mobile space, it is more important than ever for policymakers to enable strong countermeasures protecting smart devices. For this reason, Congress should reject efforts to require software platforms to allow side loading of unvetted and potentially dangerous software. In particular, we urge the Committee to oppose the Open App Markets Act (H.R. 5017 / S. 2710) and the American Choice and Innovation Online Act (H.R. 3816), which would generally prohibit software platform gating functions that prevent side loading of malware, apps that pirate content and ad revenue,[15] and other bad actors.

c. What are the most important steps Congress can take to make sure that the Federal Trade Commission can fulfill its duty to protect consumers from unfair, deceptive, and anticompetitive behavior?

RESPONSE:

Unfair and deceptive acts or practices. We urge Congress to enact a federal privacy law that preempts analogous state laws with substantially the same scope.[16] A federal privacy law should better equip the FTC to pursue privacy harms as well as impose a set of federal data security requirements.

---

[13] *Id.* at 17.
[14] Hearing on "Transforming the FTC: Legislation to Modernize Consumer Protection," before the House Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce (117th, 1st Sess.), statement of Sally Greenberg, Exec. Dir., Nat'l Consumers League (Jul. 28, 2021), *available at* https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Greenberg_CPC_2021.07.28.pdf.
[15] Graham Dufault, "Proliferation of Ad Piracy Means Platform Protections are More Important than Ever," ACT | THE APP ASSOCIATION BLOG (Aug. 13, 2021), *available at* https://actonline.org/2021/08/13/proliferation-of-ad-piracy-means-platform-protections-are-more-important-than-ever/.
[16] *See* ACT | THE APP ASSOCIATION, PROTECTING CONSUMER PRIVACY, GROWING SMALL BUSINESS (2021), *available at* https://actonline.org/wp-content/uploads/Privacy_MOC_20_21.pdf.

Anticompetitive behavior. Congress should consider clarifying the applicability of the FTC Act's prohibition on unfair methods of competition (UMC) to cases involving standard-essential patent (SEP) licensing. As part of the process of voluntarily declaring patents as essential to standards, patent holders generally agree to license SEPs on terms that are fair, reasonable, and non-discriminatory. Unfortunately, while federal law and policy generally prohibit anticompetitive licensing activities by SEP holders—especially those practices that violate SEP holder commitments to make licenses available on a fair, reasonable, and non-discriminatory basis (FRAND)—aggressive licensors continue to take advantage of gray areas in the law to gouge consumers, resulting in fewer choices, less innovation, and lower quality in the market.[17] As small mobile software and connected device companies, App Association members depend on a strong, private sector-led standards-setting system that maximizes innovation on top of foundational technologies like technical standards (such as Wi-Fi, 4G, and 5G). Congress should consider clarifying that certain SEP licensing practices constitute UMC.

[17] Brian J. Love, Yassine Lefouili, and Christian Helmers, *Do Standard-Essential Patent Owners Behave Opportunistically? Evidence from U.S. District Court Dockets* (Nov. 8, 2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3727085.

The Honorable Gus Bilirakis (R-FL)

1. Mr. Dufault, I introduced H.R. 2672, the "FTC REPORTS Act," which would require the FTC to publish and submit to Congress an annual report on the FTC's enforcement actions involving allegations of elder fraud. As you know, this Committee has a rich history of passing bipartisan legislation to go after fraudsters, including giving the FTC authority to do so. Can you speak to how important it is for the FTC to have sufficient resources dedicated to combatting fraud?

   RESPONSE:

As far as certain demographics that are especially vulnerable to online harms, statistics suggest that consumers under 25 and over 75 are also more vulnerable to online harms, especially those that result from bad actors through social engineering.[18] The FTC's own data points to fewer reports of dollar losses by older consumers but higher median losses per attack.[19] The evidence here supports action by the Committee to direct the FTC's focus on elder fraud and the FTC Robust Elderly Protections and Organizational Requirements to Track Scams (FTC REPORTS) Act (H.R. 2672) would help in this regard. Similarly, recent FTC data also indicates that members of the military community reported higher median losses due to fraud than the public at large.[20] Therefore, the Veterans and Servicemember Consumer Protection Act of 2021 (H.R. 4483) is also a welcome measure to ensure the FTC focuses its enforcement efforts on fraud schemes tailored to the military community. Lastly, as fellow witness Sally Greenberg of National Consumers League pointed out, "affinity fraud" threatens a variety of demographics, as fraudsters are known to target consumers based on their sexual identity, ethnicity, religion, race, and other protected characteristics.[21] The Consumer Equity Protection Act (H.R. 4460) is therefore a welcome measure to help direct the FTC's efforts to combat fraud schemes specifically targeting these communities.

Since fraudsters are ramping up their attacks on vulnerable populations and businesses in the mobile space,[22] it is more important than ever for policymakers to enable strong

---

[18] "Cybercrime report finds young adults and adults over 75 most vulnerable to fraud attacks," SECURITY MAGAZINE (Feb. 25, 2021), *available at* https://www.securitymagazine.com/articles/94684-cybercrime-report-finds-young-adults-and-adults-over-75-most-vulnerable-to-fraud-attacks.

[19] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 2020 13 (Feb. 2021), *available at* https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf.

[20] *Id.* at 17.

[21] Hearing on "Transforming the FTC: Legislation to Modernize Consumer Protection," before the House Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce (117th, 1st Sess.), statement of Sally Greenberg, Exec. Dir., Nat'l Consumers League (Jul. 28, 2021), *available at* https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Greenberg_CPC_2021.07.28.pdf.

[22] LEXISNEXIS RISK SOLUTIONS, FRAUD TRENDS TO WATCH IN 2021 (2021), *available at* https://risk.lexisnexis.com/insights-resources/infographic/fraud-trends-to-watch-in-2021 (indicating that attacks in the mobile space increased 48 percent in 2020).

countermeasures protecting smart devices. For this reason, Congress should reject efforts to require software platforms to allow side loading of unvetted and potentially dangerous software. In particular, we urge the Committee to oppose the Open App Markets Act (H.R. 5017 / S. 2710) and the American Choice and Innovation Online Act (H.R. 3816), which would generally prohibit software platform gating functions that prevent side loading of malware, apps that pirate content and ad revenue,[23] and other bad actors.

[23] Graham Dufault, "Proliferation of Ad Piracy Means Platform Protections are More Important than Ever," ACT | THE APP ASSOCIATION BLOG (Aug. 13, 2021), *available at* https://actonline.org/2021/08/13/proliferation-of-ad-piracy-means-platform-protections-are-more-important-than-ever/.