UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Melissa Holyoak

A PATH FORWARD ON PRIVACY, ADVERTISING, AND AI

MELISSA HOLYOAK*
COMMISSIONER, U.S. FEDERAL TRADE COMMISSION

SEPTEMBER 17, 2024

REMARKS AT NATIONAL ADVERTISING DIVISION KEYNOTE 2024

* The views expressed in these remarks are my own and do not

Thank you, Laura, for the introduction and for inviting me today. I'm delighted to be in New York today, fresh from a trip to Paris, where I had the privilege to meet with the CNIL, the French Competition Authority, and many others interested in the consumer protection and competition issues.

After traveling, I like to reflect a bit on my experience and think agy -7 -1.212 108 7082 39 nsum4 /Pag

Second, I am also concerned that the Commission has been approving civil penalty settlements based on alleged violations of Section 5(m)(1)(B) of the FTC Act,[5] even where the *sole basis* for alleging the "actual knowledge" required by this section is the receipt of a mass-mailed Notice of Penalty Offenses which describes conduct dissimilar from that of the recipient.[6] Indeed, some of the attendees of this conference may have received these stock notices related to substantiation, earnings claims, endorsements, or other topics, which provide cursory descriptions of adjudicated Commission actions, some dating from the 1940s. I am concerned that by predicating settlements merely on stock notices—[illegible]

These and other departures from what Congress has authorized are troubling for several reasons. First, exceeding our authority undermines our commitment to the Constitution. The Constitution vests authority to make laws in the Congress, not in unelected bureaucrats.[10] The Supreme Court has made clear that courts will not countenance agencies' usurpation of Congress's prerogative to make the laws.[11] We act at our peril when we ignore that fact.

My second concern is more pragmatic: where we depart from the balance carefully struck by Congress, we are more likely to get it wrong. For example, my concern with the Health Breach Notification Rule was not just that the Commission was inappropriately legislating by rulemaking, but also that its lawless reading of the statute removed any limiting principle, resulting in harmful unintended consequences and increasing the likelihood of legal challenge.[12]

As my family prepares our Wizard of Oz costumes for our neighborhood Halloween party, I am mindful of my 13-year-old son, who told me adamantly that he prefers the tin man to a straw scarecrow. In his view, it's better to have no heart than no brain. Neither tin nor straw will work here: we need both heart and mind to tackle these complex issues that have real impact on consumers' daily lives. Here are a few of the straw men we are facing.

A. "Surveillance Advertising"

Take the "surveillance" straw man. Over the past few years, the Commission has repeatedly referred to a range of data practices as "commercial surveillance."[16] Targeting advertising is "surveillance advertising."[17] Personalized pricing, the subject of the most recent FTC orders under Section 6(b) for market study,[18] is "surveillance pricing."[19] The term "surveillance" conjures nefarious action and actors—the inescapable watchful eye of Big Brother (or stealth network of Brothers) motivated by corporate greed.

Perhaps this re-branding is just silly—an attempt to boost press appeal, pander to the like-minded, score some political points—and basically harmless. But I fear that the silliness belies som0sp tsp(a)-1 (EMC-5 (e)1 (a)-2 (i)-2 (ke)0.00 (s)]Tbl2 (ous)-1 ng:)-2 (or)-2 (ag)-2 (ko ( )]T1 (ur) (ng

"bans" in FTC privacy orders are actually specific prohibitions with exceptions and consent requirements not enormously dissimilar to past Commission actions.

To be clear, as a general matter, I support a nuanced approach in FTC privacy orders in which prohibitions have appropriate, fact-specific exceptions. I am simply concerned that failing to call a spade a spade obfuscates the complexity of the issues in a manner that hampers the debate.

Rather than only nominally tossing out the "notice-and-choice" model, it may be better to frame the privacy debate in a different

C. The Rises of Data Minimization?

Data minimization gets the obverse treatment from notice and choice. Data minimization has come into fashion as the panacea *du jour*—even though data minimization has been part of the the "FIPPs," the "fair information practice principles" guiding privacy policymaking, for decades.[40] It's been a longstanding privacy principle for good reason: there can be a

It's easy to identify the wrong turns, but hard at times to find the path forward. So rather than just criticizing past actions, I would like to offer an alternative vision for the FTC's work on privacy and AI—one focused less on banning and branding and more on grappling with complexity to address harms.

With limited resources, the Commission must always triage where to dedicate enforcement efforts. As a first cut, we should be focused on tailored enforcement actions that protect sensitive personal data rather than on sweeping regulation of *all* personal data. As former Bureau of Competition Directors Susan Creighton and Bruce Hoffman put it, when fishing for law violations, "the best place to fish is where the fish are plentiful."[42] We are more likely to find harm to consumers from mishandling of children's personal data or precise geolocation data revealing consumers' political or religious activities than we are from data practices involving less sensitive information.

Indeed, these two types of sensitive data have been the subject of recent FTC actions, *NGL* and *Kochava*. In my concurring statements on these matters, I have explained the basis for my support for each.

Children and young teens are especially vulnerable online because, with their developing brains and shifting hormones, they do not always have the cognitive capacity for judicious decisionmaking.[43] As a mother of four, including tweens and young teens, I am reminded of this on a daily basis. It is crucial that we protect kids online both from bad actors and from bad judgments made easy by weak default privacy settings[44]

Confidence Act (ROSCA)[49] to shut down an anonymous messaging app aimed at children and teens that was sending fake, provocative messages (such as "are you straight?, "I stalk u on ig [Instagram] all the time", "I know what you did") to prey on tween's insecurities to lure them into buying NGL's subscription product.[50] As I noted in my statement supporting this settlement, the Commission is at its best when protecting the most vulnerable among us (children), because deception is most likely and the risk of substantial injury at its greatest where kids are involved.

I also voted in support of an amended complaint against location data broker Kochava, because the misuse of precise geolocation information revealing consumers' medical, political and religious activities presents grave dangers to the freedoms of Americans.[51] For consumers to realize the benefits of technology, they must be able to trust that technology—including tools that hold their sensitive personal data—will remain secure from wrongful government surveillance.[52] (And, here, by the way, I do in fact mean government *surveillance*, with all of its negative connotations.)

While our work must always remain within the bounds authorized by Congress, that does not mean we must necessarily take a crabbed view of harm. Undermining parental choice,[53] intruding into the sanctum of the home,[54] identity theft,[55] exposing a child to the risk of predation

Of course, as I noted in my concurring statement regarding *Kochava*, we must be responsive to judicial feedback and only take action where we have reason to believe there are legally cognizable harms.[59]

As we consider how to protect the privacy of consumers' sensitive personal information, we also need to be mindful of the effect of privacy issues and our regulatory choices on competition.[60] For example, companies with better access to data by virtue of their gatekeeper role in the digital ecosystem can have a competitive advantage. What may be pro-privacy may also be anticompetitive. Are, for example, walled gardens good for privacy but less so for competition? In 2019, the Commission under Chair Joseph J. Simons held a series of hearings on competition and consumer protection issues in the 21st century which explored some of these important issues.[61] We should learn from this past work and promote further research and dialogue to aid Congress in its consideration of privacy issues.

Similarly, we need to be mindful of the competitive effects of regulation. Regulation can create barriers to entry that may entrench the large, sophisticated companies that can bear the cost of complying with those regulations. Companies may artificially stifle growth to avoid reaching the size at which they would become subject to regulatory requirements. The Commission should not be choosing winners and losers in the market. FTC action should be market-reinforcing, not market-compromising or -replacing.[62]

Given the number and magnitude of the concerns, I understand the appeal of creating "guardrails" or "rules of the road" for AI development and use. At the same time, as I've mentioned, when we act without fully understanding the problems—and without rigorous evidence of them—we are likely to get it wrong, decreasing innovation and harming consumers and competition rather than protecting them. Of course, if Congress were to empower the FTC with authority to implement defined "AI rules of the road," I would vigorously enforce that law. But the Commission is not Congress.

Rather than speculate about harms from AI or indulge a salience bias—where we assume that a few, highly visible problems are indicative of larger-scale problems—the Commission needs to learn more about AI, such as through a rigorous 6(b) study of market practices,[64] targeted enforcement, and by promoting research and stakeholder dialogue. And we should continue to use our enforcement authority according to what we learn.

In my view, the Commission should approach AI in four ways.

First, the Commission should continue its important work to stop AI-powered fraud—that is, fraud made more effective and widespread through the use of AI. As I mentioned during an Open Commission Meeting a few months ago, the Commission's recent Voice Cloning Challenge is a great example of its efforts to stop AI-powered fraud.[65] Voice cloning can be an important medical aid for consumers who have lost their voices from accidents or illness. But, as with any technology, voice cloning can be used for good or for ill. Bad actors can use voice cloning to target individuals or small businesses via impersonation frauds, in which consumers are duped into sending money because they believe they are talking to someone they know and trust.

Earlier this year, the Commission held a "Voice Cloning Challenge," which offered a prize for innovative solutions to the threats voice cloning can pose.[66] Some winners of the challenge used AI themselves, such as algorithms to differentiate between genuine and synthetic voice patterns.[67] With efforts like the Voice Cloning Challenge, the Commission does important work to ensure that AI is used for good rather than harm.

Second, the Commission should protect consumers from deception about AI—whether it's deception about AI's capabilities, what "AI-powered" product will deliver, or something else. This summer, I voted in support of an amended complaint against FBA Machine and related entities and individuals that made false claims that consumers would earn enormous sums by investing in AI-powered online stores when, in fact, FBA Machine's products made consumers lose money and incur debt.[68] It's critically important that the Commission take action of this sort to stop deception

[64] 5 U.S.C. § 46(b).
[65] *See* Transcript of FTC Open Comm'n Meeting at 16, (May 23, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/transcript-ftc-open-commission-meeting-5.23.24.pdf.
[66] *The FTC Voice Cloning Challenge*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/contests/ftc-voice-cloning-challenge.
[67] Fed. Trade Comm'n, Press Release, *FTC Announces Winners of Voice Cloning Challenge* (April 8, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-winners-voice-cloning-challenge.
[68] Amended Compl., *FTC v. FBA Machine/Passive Scaling*, FTC Matter No. X240032 (June 14, 2024), https://www.ftc.gov/legal-library/browse/cases-proceedings/x240032-fba-machinepassive-scaling-ftc-v.

about AI so that consumers can trust and benefit from real AI and so that honest businesses can bring innovative solutions to the market.

Third, to identify and address cognizable harms that may flow from the development and use of AI, the Commission should examine, through rigorous 6(b) market studies, workshops, or enforcement, the processes companies are using to develop and use the AI in compliance with the laws the FTC enforces.[69]

Finally, it is critical that we approach AI as the market-wide issue that it is, rather than siloing consumer protection and competition concerns. If dominant firms become even more dominant in relevant markets through the concentration of AI tools and data repositories needed to build those tools, we should examine those practices carefully.

Thank you, and I look forward to your questions.

[69] *Cf.* Holyoak Coulter Statement.