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

Office of Commissioner
Rebecca Kelly Slaughter

Disputing the Dogmas of Surveillance Advertising
National Advertising Division Keynote 2021

Remarks of Commissioner Rebecca Kelly Slaughter[1]
As Prepared for Delivery

October 1, 2021

Good morning, everyone! Thank you, Mary, for that introduction and for inviting me here to deliver these keynote remarks. I'm excited to have a chance to discuss NAD 2021's

II. Notice and Choice Is Not the Answer

That brings me to the second assumption I would like to challenge: that we can solve for data abuses by providing consumers with more transparency and control—in other words, more notice and choice. For too long, the policy debate around data collection and abuse has hinged on the principles of notice and choice and whether corresponding opt-in or opt-out rules should govern data collection. The notice-and-consent framework began as a sensible application of basic consumer protection principles to privacy—

pervasive data collection. For example, ads in mobile apps and websites drain consumers' phones' battery life and may make them pay more in phone bills.[15] Lengthy explorations of these kinds of harms have been catalogued by consumer advocates,[16] academics,[17] and even FTC commissioners.[18]

Just last week, we saw another report that shocked the conscience about the dangerous consequences of the surveillance business model. The Wall Street Journal reported that Instagram made body image issues worse for one in three teenage girls, fueling disorders, mental health crises, and self-harm.[19] And, even worse, Facebook knew that was the case. The statistic came from their own internal research.

Each of these problems merits investigation as potential violations of the law, especially the unfairness prong of the FTC Act. And none of them would be addressed by more notice and choice.

Consumers seem to be expressing their dislike with this system in every poll they can. According to Consumer Reports, 75 percent of Americans think that the power of platforms is a major or moderate problem; most Americans think they are not getting objective and unbiased search results when shopping for information online; and 81 percent of Americans are either very or somewhat concerned about the amount of data platforms hold on them to build consumer profiles.[20] A Deloitte survey indicated that an even higher number of Americans, over 90 percent, agree to the terms and conditions on mobile apps without reading them.[21] Pew paints a

---

https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[15] Craig Silverman, This Giant Ad Fraud Scheme Drained Users' Batteries and Data by Running Hidden Video ads in Android Apps, BUZZFEED NEWS (Mar. 21, 2019), https://www.buzzfeednews.com/article/craigsilverman/in-banner-video-ad-fraud.

[16] .

similar picture: 81 percent of Americans feel as if they have little control over the data companies collect and believe the risks of that data collection outweigh the benefits.[22]

I share that view. We are all surveilled, tracked, targeted—some of our communities more than others—and too often our choices are manipulated and limited. This is not the result of the expression of informed preferences in a well-functioning marketplace. Large intermediaries dominate data markets, and consumers are not able to exercise meaningful choice with respect to how their data is collected, used, and shared. Last year, the New York Times ran a powerful article by Kashmir Hill, the title of which says it all: "I tried to live without the tech giants. It was impossible."[23] As federal enforcers, it is incumbent on us to identify the unfair, deceptive, and anticompetitive practices that are harming consumers and to use all of our statutory tools to strategically and structurally address illegal conduct.

The pervasive natule

information companies can permissibly collect isn’t used to build tools or services that imperil people’s civil rights, economic opportunities, or personal autonomy.

Minimization is not a new concept, and I will be the first to acknowledge that the term comes with some baggage f

idea of data minimization seriously, though COPPA has a minimization provision,[27] as does GDPR.[28] But the concept can be extended more broadly.

Consumers ought to be able to make sensible decisions about the products they want to use and companies should ask them only for the data required to provide the products and services they actually ask for—not additional data to build consumer profiles. There also ought to be strict limits on how that information is shared and for how long and under what conditions it's stored.

Additional limitations on how data are used can also prevent abuse. Our personal information should not be used by companies to exacerbate economic inequality, segregation, further marginalize workers or deepen other disparities, whether intentional or not. Just as the government's use of huge datasets to build profiles of citizens violates civil rights and liberties,[29] widespread commercial collection can imperil freedom. And minimizing commercial data collection is inherently protective of civil liberties, too: Governments can't acquire information on Americans that no one collected in the first place.

A minimization framework would not outright ban surveillance advertising, but it would eff [(o)1 (n)1 0.002 Tc -0 (m)8 (i)-2 (ni)-7l or nuGttsabn t iTc -0.001egasza (o e)4 (xa)-1 (c)-1 (e)-1 -1 (

market despite its purported intention of protecting user privacy.[31] But minimization can be an important tool in the solutions toolbox.

IV. Limiting Surveillance Will Not Break the Internet

I suspect that the reason so much of our attention has been focused on legal and policy remedies that do not address the underlying surveillance business model is a sense that the business model is necessary for the survival of the many ad-supported businesses that populate our digital economy. This is another myth that merits busting.

Let me be very clear: I am not challenging the business models of ad-supported services. We have a rich tradition in this country of services being provided for free to consumers in exchange for their eyes and ears—advertising; television, radio, and newspapers are front of mind in that category. The difference between traditional ad-supported models and the current surveillance model is that the new model trades consumer data for a service, not just their attention. And those data are, in turn, used to fuel broader surveillance systems.

Advertising is necessary, and it should give consumers clear and accurate information about the products and services that they may want to buy. But no part of that goal requires siphoning consumer data, building extensive profiles on them, or selling that information to even less regulated third parties.

There is a better future for the ad-supported internet. One that respects people's rights and doesn't exacerbate already worsening social inequalities. Good advertising serves a real purpose; it existed before pervasive tracking and behavioral advertising and will exist after it. Good advertising can be targeted; of course an advertiser wants to make sure her product reaches the target audience efficiently. But targeting can be done contextually, triggered by the content to which an ad is attached, or even through broad and general categories. These types of targeting do not raise the same concerns that surveillance advertising does.

If surveillance advertising went away, would consumers really lose access to clear and accurate information? Or could the internet be a better place?

The New York Times' experience in Europe may be unique, but it's certainly worth considering. According to news reports, in order to comply with GDP9 (t)-w 10bg2-9 0 Td (r)-1 (n)-1 ((ng

that data regulation merely shaves off low single-digit revenues for online publishers, then we really must consider the balance of fairness in ending an abusive system on one side and marginal reductions in revenue on the other. It also not clear to me that we can get a reliable analysis of the value of surveillance advertising in a universe where some advertisers are using it and some are not because the control group distorts the field. In other words, if we are considering a model where behavioral microtargeting is not available to any advertisers, all advertising would be on a level contextual playing field.

V. The FTC Can Lead the Way Forward on Data Minimalism

So how do we get from the market morass we have today to a brighter data future? This brings me to the final myth I'd like to bust, which is that federal legislation is necessary to effectuate any of the changes I've floated. To be clear, federal legislation would be great; I have long supported federal privacy (or, as I would prefer, data abuse) legislation that would set forth clear rules of the road, explicitly empower the FTC to police abuses and adapt to changing market conditions, and impose real penalties for failure to comply. But in the absence of federal legislation, we cannot sit idly by. The FTC does have tools, albeit imperfect ones, to tackle data abuses.

First, we can target for enforcement unfair practices that exploit the fundamental asymmetry between individuals and corporations in this system. As a reminder, our standard for proving conduct is unfair under Section 5 is that (1) it causes or is likely to cause substantial injury, (2) the injury is not reasonably avoidable by consumers, and (3) the injury is not outweighed by benefits to consumers or to competition.[33] In addition to targeting unfair conduct with respect to data, w4cbv1 (w)3 (4ct w)3 (4cct)-1 c3o cot d (w)3 (ar)1 (a(co)6 (4 (.)1 (f)4 (as)]TJ

do otherwise would be ignoring the will of Congress. And, finally, that argument is premised on