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

Office of Commissioner
Rebecca Kelly Slaughter

Wait But Why? Rethinking Assumptions About Surveillance Advertising
IAPP Privacy Security Risk Closing Keynote 2021

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

October 22, 2021

Good morning, everyone! It is a pleasure to be here today to close out a busy week of grappling with some of the most pressing issues in the data economy. I am going to use my time this morning to provide you some food for thought as you leave this conference about what the future of data might look like, and try to provoke some new ways of thinking about a very important area of the law.

As you all know, we are in the middle of a major transition at the FTC; of course we have had changes in personnel and leadership, but we are also changing our perspective, and approaching our mission with open eyes about what has been working and where we need a new direction. An important part of keeping our work fresh and effective is challenging assumptions—whether recently developed or longstanding—about everything from market operation, enforcement objectives, and the agency's strategic approach. This is what I refer to in my office as the "Wait, but why?" model of analysis. Too often, we can do an expert job of explaining *how* we analyze particular cases or *what* our strategy is, but not *why* we do it that way. And when we step back and ask, "wait, but why?" we frequently uncover areas in need of a dramatic rethink. So, I'd like to frame my remarks today around assumptions that I believe are particularly in need of challenge in the data surveillance ecosystem.

Specifically, I want to push back against the following erroneous points of conventional wisdom that I think tend to undergird the legal and policy debate about digital surveillance: (1) privacy is the key issue; (2) transparency and choice are the key solutions; (3) the policy options are limited to opt-in or opt-out; (4) surveillance advertising is necessary to support free services; and (5) the FTC is toothless absent new federal legislation. All of those statements, which I've heard repeatedly presented as truisms, have obvious flaws on closer examination. Today, I want not only to explain why I believe they are flawed but also to outline a vision for an ad-supported internet future that is better grounded in the realities of today's markets and the law.

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other commissioner.

I. Why are we just talking about privacy?

Yesterday, the FTC released a staff report addressing the data practices of major ISPs, the product of a 6(b) study that was launched in 2019.[9] Our ISP report highlighted the ways in which data collected by ISPs "could be used in a way that's harmful to consumers, including by property managers, bail bondsmen, bounty hunters, or those who would use it for discriminatory purposes."[10] Of course, this is not just about ISPs; the same problems can arise whenever data is indiscriminately collected, compiled, and shared.

I want to dwell for a moment on the ways in which data surveillance can be harmful from a civil rights and equity perspective. The ISP report provides a great example of the ways data can be collected and compiled to facilitate targeting based on protected class status. The report explains that ISPs combine data they collect with data they source from brokers to put customers into segments.

> These segments often reveal sensitive information about consumers. Examples of such segments include "viewership-gay," "pro-choice," "African American," …"Jewish," "Asian Achievers," "Gospel and Grits," "Hispanic Harmony," "working class," "unlikely voter," "last income decile," "tough times,"… These categories allow advertisers to target consumers by their race, ethnicity, sexual orientation, economic status, political affiliations, or religious beliefs, raising questions about how such advertising might (1) affect communities of color, historically marginalized groups, and economically vulnerable populations, or (2) reveal sensitive details about consumers' browsing habits.[11]

I am particular about using the right framing because the appropriate identification of a problem is key to the effective tailoring of solutions. If we are concerned only about privacy—the sharing of personal information without knowledge or consent—we may narrowly focus on solutions that address only that knowledge and consent, such as burdensome opt-in or opt-out frameworks, and not look at the economy and society-wide implications of unfettered data collection used to fuel surveillance advertising.

Instead, I'm interested in seeing us squarely target the business practices that I think are the source of so much harm.

II. Why do we focus so much on notice and choice?

That brings me to the second question: can we really solve for data abuses by providing consumers with more transparency and control—in other words, more notice and choice? I don't think so.

The notice-and-choice framework began as a sensible application of basic consumer protection principles to privacy: tell consumers what you are doing with their data, secure consent, and keep your promises. It also has some intuitive appeal, because it sounds like it is providing users with more autonomy.

Historically, this is how much of the FTC's data privacy work operated, through cases against companies that misled users about what was happening with their data in violation of the deception prohibition in the FTC Act. In those cases, a tell-the-truth remedy might seem apropos: Be honest with users about what you are doing with their data, and you will be fine. But that approacta, asuasP1 (nd ncb (s)4 (MCID 14 ≥.44 0 Tdl)3 (a)-8.t (s)4 (MCI (MCID 14 ≥Tjw)2 (i)-2 (t)-2 (h us)-gM

a T (n 0 3 d 8 l a i - - p .

putting up your geolocation information for sale.[24] Studies show that even idle smartphones transmit undisclosed amounts and types of information to their manufacturers.[25]

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. The lack of meaningful competition makes the notice and choice problems even worse. Large intermediaries dominate data markets, and consumers can't exercise meaningful choices 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."[26] 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 nature of commercial surveillance, its substantial injuries to consumers, its unavoidable nature, and the paucity of benefits that outweigh those injuries demonstrate a fundamental unfairness at the heart of the data economy.

That's the crux of the issue with the status quo: a data regime built entirely on notice and choice will perpetuate this unfairness because it accepts as a baseline the idea that companies are entitled to collect vast amounts of user data as long as they are honest about it.

III. Why don't we look at other models?

That brings me to the next assumption I would like to challenge: the idea that we are stuck with notice and choice as a framework, with the operative question being opt-in or opt-out for different types of data. Understanding that the collection itself fuels the panoply of problems under the umbrella of "data abuses" helps point to a potentially more effective solution: bright-line purpose and use restrictions that minimize the data that can be collected and how it can be deployed.[27] This data minimization approach would turn off the data pump and deprive the surveillance-economy engine the fuel it needs to run.

Fundamentally, data minimization should mean that companies collect only the information necessary to provide consumers with the service or product they actually request and

---

[24] Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller and Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES, Dec. 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[25] Douglas J. Leith, *Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google*, Teve(t)0.6 (g)1(o)]TJ0 T.2 (i)0.6 (i)-5.4 (m-5 (ecs)-2.3 (s)3.8 (.3 (r)45.5 (a)6 (glT.2 p0.5 (e)-1.1 (m-5 (e)]TJ0 T1)0t)11.6 i)0.5 (p)-5 (s)

use the data they collect only to provide that service or product.[28] Data minimization should be coupled with further use, purpose, sharing, and security requirements to ensure that the

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.

As the ISP report discussed, indiscriminate collection and sharing invites abuse. Our personal information should not be used by companies to exacerbate economic inequality or 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,[32] 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 effectively disable it. If companies cannot indiscriminately collect data, advertising networks could not build microtargeting profiles. Without the monetization aspect of microtargeting, the incentive to indiscriminately collect data falls away.

Finally, a minimization approach could facilitate compliance by establishing bright-line rules around what data can be collected and how it can be used. That will allow us to move past the compliance exercise of interminable and unreadable click-through terms of service contracts that only give the illusion of meaningful notice and choice.

Of course, addressing the myriad concerns posed by the surveillance economy requires a multifaceted approach, especially attention to competition.[33] But minimization can be an important tool in the solutions toolbox.

IV. Why do we need micro-targeting?

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 place to ask "wait but why?"

---

[32] Tim Lau, *Predictive Policing Explained*, BRENNAN CENTER FOR JUSTICE, Apr. 1, 2020, https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

[33] Corporate self-dealing is also a serious problem in the data ecosystem, and, as long as key digital markets are controlled by just a few large, data-hungry online platforms, both consumers and prospective entrants are at their mercy. As Public Knowledge's Charlotte Slaiman discussed in her recent Senate Judiciary testimony, decisions by gatekeepers such as Facebook can have dramatic effects on publishers, as happened in Facebook's "pivot to video." Similarly, Google's decision to block third-party cookies in Chrome while launching a privacy sandbox could mean an even stronger grip by the company on the internet advertising market despite its purported intention of protecting user privacy. Charlotte Slaiman, *Testimony of Charlotte Slaiman, Competition Policy Director, Public Knowledge, Before the United States Senate Committee on the Judiciary, Subcommittee on Competition Policy, Antitrust, And Consumer Rights for the hearing on Big Data, Big Questions: Implications for Competition and Consumers* 5– 6, Sept. 21, 2021, https://www.judiciary.senate.gov/imo/media/doc/Slaiman%20Testimony.pdf.

Let me be very clear: I am not challenging the business model 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 on advertising: television, radio, and newspapers. The difference between traditional ad-supported models and the current surveillance model is that the new model trades consumers' *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 or use. 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 could be a better future for the ad-supported internet. One that respes-2 (n-f6. 6 0 Td( )Tj0.00n-1 (g

ending an abusive system on one side and marginal reductions in revenue on the other. We cannot just assume that some value to one group is a necessary price to pay for harm to another, especially if there is a less harmful way to provide a substantial portion of the advertising value.

V. Why do we need to wait for Congress to act?

So how do we get from the market morass we have today to a brighter data future? This brings me to the final assumption I'd like to challenge, 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.[35] In addition to targeting unfair conduct with respect to data, we can also ensure that we are tailoring remedies to get to the ro(o)1 5hf-2 (ab)1 (u)11)t rir

In addition to our investigatory tools we have the opportunity to develop a public, participatory record and use it to draft rules that let businesses know what Section 5 means in the context of the data economy. We can show how our understanding of what is unfair has evolved in response to these prevailing market practices. We can give specific guidance to industry about the requirements of the law that will facilitate compliance and streamline the Commission's enforcement burdens, allowing us to use our limited resources more efficiently.

Of course, I have no certainty that a rulemaking record would support a minimization rule or any other particular approach; I am mindful of the legal and prudential need for the agency to follow the facts and evidence where they lead. But I am confident that it is time for us to start asking the questions and developing the record, before the practices we've discussed and investigated become even more entrenched.

The market is changing whether we promulgate rules or not. People are complaining to pollsters,[36] but they are also taking action. As we've all seen with Apple's mobile changes, consumers, when given the choice, will elect not to be tracked in numbers that are sending shockwaves through industry.[37] But I do not want to see an internet ecosystem fully controlled by one or two device and operating system manufacturers; that raises very real competitive concerns. Shutting off the data spigot for others while filling your own well is the kind of anticompetitive innovation that we're bound to see more of if this space remains unregulated.[38]

That's why I see a fairer and more equitable future in leveling the playing field for advertisers, service and product providers, and operating system manufactures alike. Bright-line