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?

The first question I would like to pose is why do we focus so much on privacy as the primary concern for consumers in data-driven digital markets? Of course, privacy is critically important—I share the view that it is a fundamental right. But it is not the *only* important concept either as a matter of law or as a matter of values when it comes to the data economy. I worry that, when we focus exclusively or even primarily on "privacy," we can exclude from our gaze other critical issues people face in digital markets.

I may sound like a broken record on this point; I've been beating the "not just privacy" drum for several years.[2] And, indeed, our work at the FTC has already moved past narrow traditional "privacy" problems like dishonest terms of service for data use. We've issued guidance on algorithmic bias,[3] explored "dark patterns" in user-interface design,[4] and gone after companies that have sold sensitive information such as Social Security numbers to other companies that had no legitimate business need for the information.[5]

I'm concerned that a market based around leveraging massive amounts of people's data generates harms that extend well beyond traditional privacy concerns, particularly: harms to civil rights and equal opportunity, the proliferation of misinformation, harms to competition, and increasing labor exploitation, including through worker surveillance.

The practice of nearly unconstrained data collection, retention, and sharing can be harmful to consumers. Overcollection encourages leveraging huge amounts of data as a surveillance business model and then turning those data into products, some of which have, among other problems: increased the severity of data breaches;[6] fueled misinformation campaigns;[7] or exacerbated mental health problems among teenagers.[8]

---

[2] Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law,* Silicon Flatirons-University of Colorado Law School, Sept. 6, 2019, https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf

[3] Elisa, Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC, April 19, 2021, https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

[4] *Bringing Dark Patterns to Light*, FTC, Apr. 29, 2021, https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop.

[5] Compl., *FTC v. Blue Global, LLC*, No. 2:17-cv-02117-ESW (D. Ariz. filed July 5, 2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3225/blue-global-christopher-kay.

[6] Whitney Lance, *2020 Sees Huge Increase in Records Exposed in Data Breaches*, TECH REPUBLIC, Jan. 21, 2021, https://www.techrepublic.com/article/2020-sees-huge-increase-in-records-exposed-in-data-breaches/.

[7] *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia's Use of Social Media with Additional Views,* Select Committee on Intelligence United States Senate, Nov. 10, 2020, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[8] Georgia Wells, Jeff Horwitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J., Sept. 14, 2021, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739. There are also less dramatic harms of 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. Craig Silverman, *This Giant Ad Fraud Scheme Drained Users' Batteries and Data by Running Hidden Video ads in Android Apps,* BUZZFEEDNEWS, Mar. 21, 2019, https://www.buzzfeednews.com/article/craigsilverman/in-banner-video-ad-fraud.

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]

Of course, ISPs are not the only companies leveraging data in ways that potentially violate civil rights; there is ample documentation of data being used to reproduce patterns of discrimination against protected classes in areas of key economic opportunities.[12] Lengthy explorations of these kinds of harms have been catalogued by consumer advocates,[13] academics,[14] and even FTC commissioners.[15]

Each of these problems merit investigation as potential violations of the law, especially the unfairness prong of the FTC Act, even though they do not fall within the ambit of "privacy" as it is generally conceived. But they also cannot be separated from the traditional privacy problems entirely; all stem from the same indiscriminate data collection. I implore us to think about these problems collectively as "data abuses" rather than force all these issues under the privacy umbrella.

---

[9] *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, FTC (October 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf

[10] FTC, supra note 7 at iv.

[11] *Id* at 22.

[12] *See* Yeshimabeit Milner & Amy Traub, *Data Capitalism and Algorithmic Racism*, DEMOS, May 17, 2021, https://www.demos.org/research/data-capitalism-and-algorithmic-racism.

[13] *Civil Rights and Privacy Letter,* Aug. 4, 2021, https://cdt.org/wp-content/uploads/2021/08/2021-08-04-FTC-civil-rights-and-privacy-letter-Final.pdf.

[14] Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, George Washington School of Law, 2021, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2790&context=faculty_publications.

[15] Rebecca Kelly Slaughter, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, YALE JOURNAL OF LAW & TECHNOLOGY, Aug. 2021, https://yjolt.org/sites/default/files/23_yale_j.l._tech._special_issue_1.pdf.

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 approach simply doubles down on a notice-and-choice universe in which neither notice nor choice is meaningful for most users.

Notice happens mostly in the form of lengthy click-through contracts. Few consumers can dedicate the time and legal parsing required to understand them.[16] And choice is illusory at best. Users do not actually have bargaining power—even if they could read and understand the lengthy terms of contracts they must sign, their options are only to agree or to refuse and be denied access to the services that power modern life. Given limited competition in the marketplace, the choice to decline may not be a viable one. Choice is fallacious in other ways as well: Many sites are designed to optimize the number of "opt-ins," including through dark patterns, where tricks are employed by designers or developers to make users do something they otherwise would not want to do. In other words, what feels like "choice" may in fact be the product of manipulation.

Our ISP report provided a clear example of the flaws of notice and choice. ISPs "promise consumers that they 'will not sell your personal information,' providing an impression that their

[16] A widely cited article calculated that it would take a consumer 76 work days to read all the privacy policies she encounters each year. Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

information will not be used or transferred for unanticipated purposes."[17] Nonetheless, the report explains, "Many of these ISPs give insufficient information to consumers regarding the myriad of ways that their data can be used, transferred, or monetized outside of selling it, often burying such disclosures in the fine print of their privacy policies."[18] In addition, the report reflects that even purported choices around data are simply "illusory."[19]

But, even if we imagined a hypothetical universe in which notice and choice were actually meaningful, they would still be problematic because they put all of the burden on users to protect their data even though those users have very little control over that data. Companies can and do track consumers across their devices and locations, and data about consumers are shared, sold, or used for targeting. Much of this happens between and among companies with which consumers never choose to interact – again, see our ISP report for some clear examples.[20]

Notice and choice will not address the broader surveillance practices upon which the current digital advertising economy is built. As our ISP report noted:

> While consumers certainly expect ISPs to collect certain information about the websites they visit as part of the provision of internet services, they would likely be surprised at the extent of data that is collected and combined for purposes unrelated to providing the service they request—in particular, browsing data, television viewing history, contents of email and search, data from connected devices, location information, and race and ethnicity data.[21]

Of course ISPs are not the only example of overcollection; consider the paradigmatic example of the "Brightest Flashlight Free" app which collected and shared user geolocation data even though the service offered to consumers was simply turning on and off their phone's camera flash LED.[22]

Why would these companies need or want to collect data totally unrelated to their services? Monetization. This is a pattern we see all too often across the digital economy. Too many services are about leveraging consumer data instead of straightforwardly providing value. For even the savviest users, the price of browsing the internet is being tracked across the web.[23] Connecting with your community on social media or ordering delivery on your phone can mean

---

[17] *Id.* at 26.
[18] *Id*.
[19] *Id* at 27.
[20] John Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, THE MARKUP, Sept. 30, 2021, https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data; FTC, supra note 7, at 25.
[21] FTC, supra note 7, at iv.
[22] The app's collection of geolocation information had nothing to do with the service on offer—activating the camera flash for illumination. Consumers had no reason to think their geolocation information would have been sent to advertising networks. The FTC brought a case against the app developer based on failure to disclose that collection, but there is no reason to think most consumers would have been meaningfully aware of that collection or data transfer even if it had been disclosed in the app's terms of service. *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, FTC, Dec. 5, 2013, https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.
[23] Farhad Manjoo, *I Visited 47 Sites. Hundreds of Trackers Followed Me*, N.Y. TIMES, Aug. 23, 2019, https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html.

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*, Trinity College Dublin, Mar. 25, 2021, 1 n.1 ("We note that at the bottom of the Google text beside the 'Usage & Diagnostics' option it says, 'Turning off this feature doesn't affect your device's ability to send the information needed for essential services such as system updates and security.' Our data shows that the 'essential' data collection is extensive, and likely at odds with reasonable user expectations."), https://www.scss.tcd.ie/doug.leith/pubs/apple_google2.pdf.

[26] Kashmir Hill, *I Tried to Live Without the Tech Giants. It Was Impossible*, N.Y. TIMES, July 31, 2020, https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html.

[27] Data minimization is a concept grounded in the Fair Information Practice Principles. *See* IAPP, *Fair Information Practice Principles,* https://iapp.org/resources/article/fair-information-practices/.

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 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 from its alternative life in the national security space. In that sphere, data can be collected only pursuant to standards such as "reasonable articulable suspicion" for certain investigations, without which collection is unlawful. Additional processing, analysis, dissemination, and retention of the information must also be minimized. That means national security agencies are largely prevented from collecting or disseminating U.S. person information that isn't related to an investigation; they must promptly destroy records they acquire that don't contain relevant intelligence information; and information that is relevant can be retained only for a limited time prescribed by law.[29]

Commercial law for the most part hasn't taken this idea of data minimization seriously, though COPPA has a minimization provision,[30] as does GDPR.[31] But the concept can be extended more broadly.

Now, I know that important work is still being done to reform and oversee the national security programs. We don't have to use the word minimization, because perhaps the term is too weighted down with its failure to live up to its promise in the national security space; we could talk instead about "purpose and use limitations." But for now I'm going to stick to minimization, not only because "purpose and use limitations" is a mouthful.

The concept of minimization is a valuable one, reflecting important understandings that can translate to the commercial space. Among those: Collectors of information hold enormous power. Without oversight, abuse is nearly inevitable. Data collection must have limits. Data should only be collected for discrete and specific purposes. We should be extremely skeptical about secondary uses of data—that is, uses beyond the purpose for which the data was collected. Collection and use limitations can help protect people's rights.

We should approach commercial surveillance and use of our data with the same seriousness that we have in the national security environment. It should not be necessary to trade one's data away as the cost of full participation in society and the modern information economy.

---

[28] *See* Eric Null, Iseuda Oribhabor & Willmary Escoto, *Data minimization: Key to protecting privacy and reducing harm*, ACCESS NOW, May 20, 2021, https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf.

[29] *See Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, https://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

[30] *Complying with COPPA: Frequently Asked Questions,* FTC, July 2020, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0.

[31] Article 5(1)(c) of the European Union's General Data Protection Regulation, https://gdpr-info.eu/art-5-gdpr/.

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 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?

One of the underlying questions here is how much value does micro-targeting provide, and to whom? I have heard frequently the assertion that it provides substantial value to both advertisers who are better able to reach a target audience and to publishers who host ads, by raising the price advertisers are willing to pay. But I have yet to see evidence that either of these propositions are true. In fact, what limited evidence there is suggests that non-tracked ads can work to ensure a vibrant internet.[34]

It's 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.

But ultimately, even if we can uncover evidence holds that limiting targeting shaves off degree of value for advertisers and publishers, we still must consider the balance of fairness in

[34] 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 GDPR, the Times blocked open-exchange ad buying on its European pages and followed that by blocking behavioral targeted advertising and didn't see ad revenues drop. There's good news for smaller publishers too. A 2019 study showed that behavioral advertising only led to around a 4% revenue increase to publishers over non-cookie based advertising. This study belies advertiser claims that regulation of the data ecosystem—turning off the data spigot—will harm a vibrant publishing marketplace online. Veronica Marotta, Vibhanshu Abhishek & Alessandro Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis* 7 (May 2019), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

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 root causes of the illegal conduct. For example, we could pursue minimization terms in our orders, including limitations on collection of data and deletion requirements.

But one-off enforcement cases have their limits in disciplining the market and fundamentally changing business practices. Promulgating clear rules in this area would be beneficial to consumers and businesses alike. Although it is much maligned, the FTC does have rulemaking authority under Section 18 of the FTC Act to address prevalent conduct that is unfair or deceptive. The process begins with an advance notice of proposed rulemaking, which asks important questions and builds an evidentiary record off of which a rule or several rules can be developed. We should start down that path.

I have frequently heard arguments from industry representatives and even some of my colleagues that rulemaking in the data space would be inappropriate for the FTC, because it necessarily involves value judgments that are better left to Congress. This argument rings hollow with me. First of all, by choosing not to act, we are exercising a value judgment that the market is working absent intervention. Second, it is incumbent upon us to use the tools Congress explicitly gave us—which include rule-writing authority—to carry out our statutory mission. To do otherwise would be ignoring the will of Congress. And, finally, that argument is premised on the mistaken assumption that we can, by "regulatory fiat," as one of my colleagues has said, make illegal conduct that is otherwise within the bounds of the law. Not so. We can only write rules that address conduct that already violates the FTC Act; the benefit of rulemaking is to provide clarity to the markets about what that proscribed conduct is, rather than waiting until after a violation—and the resultant harm—has occurred to redress it.

[35] 15 U.S.C. § 45(n).

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 rules can be a clear articulation of where the law stands on what are unfair or deceptive acts under our Section 5 authority. We must think clearly about what's actually necessary to make the benefits of technological progress possible and commit to doing away with the needless exploitation of people's data that imperils the free functioning of markets, our autonomy, and our rights.

---

[36] 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. *Platform Perceptions Consumer Attitudes on Competition and Fairness in Online Platforms,* CONSUMER REPORTS, Sept. 24, 2020, https://advocacy.consumerreports.org/wp-content/uploads/2020/09/FINAL-CR-survey-report.platform-perceptions-consumer-attitudes-.september-2020.pdf. 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. *2017 Global Mobile Consumer Survey US edition*, Deloitte, at 12, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf. Pew paints a 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. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER, Nov. 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[37] Alex Kantrowitz, *Apple's power move to kneecap Facebook advertising is working*, CNBC, Sept. 24, 2021 https://www.cnbc.com/2021/09/24/apples-ios-changes-hurt-facebooks-ad-business.html.

[38] *See* Garrett Sloane, *What Apple's Iphone Update Means for the Ad Industry*, ADAGE, Sept. 16, 2021, https://adage.com/article/digital-marketing-ad-tech-news/what-apples-iphone-update-means-ad-industry/2366001.