anonym

**Written Testimony of:**
Graham Mudd
Founder & Chief Product Officer
Anonym, Inc

**Hearing:**
*Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy*
House Subcommittee on Innovation, Data, and Commerce
March 1, 2023, at 8:30 AM

Chairman Bilirakis, Ranking Member Schakowsky, and distinguished Members of this Committee, thank you for the opportunity to testify at this important hearing.

My name is Graham Mudd, and I am co-founder and chief product officer of Anonym, Inc., a privacy-technology company that is focused on solving the privacy challenges facing digital advertising. My colleague and fellow cofounder, Brad Smallwood, who also is here with us today, is our chief executive officer. We're here, however, not to pitch our company–although we hope to talk a bit about what we're doing in privacy tech–but to show our support for reintroduction of the bicameral, bipartisan American Data Privacy Protection Act (ADPPA), which we believe would create a comprehensive privacy framework that would benefit all American consumers.

So, I want to begin by thanking you all–and particularly Chair Rodgers and Ranking Member Pallone of the Energy and Commerce Committee for their groundbreaking work in the last Congress–for introducing this comprehensive framework designed to set higher standards for protecting American data privacy. We at Anonym share your belief that the ADPPA has the potential to mark a historical watershed in privacy law and policy. This legislation, we believe, will reform data-privacy practices – and at the same time it will promote the ethical use of data that supports the evolution of stronger digital services.

My co-founder and I have been part of the development of the internet advertising ecosystem since the first wave of the internet in the late 1990s. Prior to Anonym, we both worked at Meta for more than 10 years, where we helped build and run the advertising business. We ran teams responsible for building the products that marketers leveraged to deliver and measure their advertising. Prior to that, we worked in product and analytics roles at Yahoo and other firms.

In all of our roles over the past 25-plus years, consumer behavioral data was an incredibly powerful asset in building more relevant products for people and more effective advertising solutions for businesses. As a result, acquiring data and putting it to use in increasingly sophisticated ways was always a strategic imperative. However, over the years, a tension began to emerge – the development of the rich consumer profiles that were so powerful in improving products of all kinds came at the cost of individuals' privacy. This trade-off is why we're here today.

We started Anonym with a simple goal – to provide technical privacy protections to consumers while at the same time ensuring that businesses continue to have the tools they need to grow. In effect, our goal is to reduce the trade-off cost of becoming a more privacy-safe digital ecosystem.

But technical protections alone are not sufficient. That's because without regulation and strong enforcement there is little incentive for companies to stop leveraging individuals' data to enhance their business.

**How Did We Get Here?**

To chart a path forward, it's often useful to reflect on what led to the status quo. Media companies have always strived to put the right information in front of their consumers. This competition for relevance – whether focused on content or advertising – has benefited consumers tremendously. Until the explosion of the internet at the turn of the century, almost all media were broadcast. Producers and editors curated content to ensure that it was relevant to the audience they were serving. Advertisers used audience research to understand the demographic makeup of these audiences so they could place their ads where their target customers were likely to see them.

Digital advertising initially relied on the same approach. Advertisers used audience research to understand the demographics of the visitors to web sites or sections of sites, like Yahoo Sports. Just as with TV, radio and print, advertisers ran ad campaigns based on informed generalizations. There were of course exceptions, like direct mail, which has always harnessed individual-level data. In fact, political campaigns were among the earliest users of detailed data for content and advertising delivery.

But then internet search changed everything. Search-based advertising for the first time allowed companies to segment their audience at scale efficiently, and importantly, match the advertising to a consumer's interests and behaviors. The opportunity to use the information about what a consumer searched for to target advertising was game changing to advertisers, consumers, and search providers alike.

Other digital publishers and ad platforms that served display advertising (e.g. banner ads) weren't as naturally blessed with the rich consumer data search providers had. To compensate, display platforms sought ways to generate and aggregate consumer data from as many sources as possible and build rich consumer profiles with it. Ad networks collected browsing and ad-click data from tens of thousands of publishers. Data brokers, who had previously focused on direct mail, began selling data to digital display-ad platforms Finally, social media companies began accumulating vast user bases – and since their users were required to log in, building rich profiles was much easier, given their access to highly accurate consumer identity data. To further extend their ability to collect, measure, and improve ad performance, many major ad platforms begin using "pixels" to collect data from across the web.

## A Pixel is Worth a Thousand Words

Pixels, and their mobile-app equivalent, tracking SDKs, are an elegantly simple yet massively powerful set of technologies, so they're important to understand. At the most basic level, pixels are small pieces of code that look for a "cookie" to identify a device or user. They are deployed by a specific ad platform to many websites and apps that they don't own or control. When a person visits a website with a pixel installed, the pixel sends data about the user's behavior on that website back to the ad platform, where it is then typically associated with that user's profile.

I'll share a recent personal example to make this all a bit more concrete. My wife and I are in the process of completing a few home renovations. As a result, I've spent a fair bit of time on home improvement sites like Home Depot. For the past few weeks, I've seen ads across the web for products I've researched (and sometimes bought) as well as many I haven't but might be interested in. Behind the scenes, pixels are at work. Home Depot has more than a dozen tracking pixels on its web site. Those pixels pass my browsing and buying behavior to ad platforms. Those platforms then use that data in their ad products. This pixel-based approach to data sharing creates value for a number of parties:

- First, and most obviously, Home Depot wins because they measure the performance of their ads by understanding which ads led to purchases on their site. Home Depot can also improve the performance of its campaigns by running highly targeted ads.
- Ad platforms win because they earn more for ads that work better. They're also able to enrich their profile of me, which allows their machine learning algorithms to deliver more effective ads for not just Home Depot, but for all of their advertising customers.
- I'm arguably a winner too, because ad platforms show me ads that are more likely to be relevant to me. Thanks to the exchange of data about my interests, I will now see more home improvement ads instead of ads for products and services that either seem randomly selected,

or that may be cued by something less relevant, like the particular content of the page I happen to be visiting.

Of course it’s not all upside. While most Americans quite reasonably haven’t spent the time to understand the mechanics at play, they know full well that their data is being shared – and most people are uncomfortable with this fact. While it may be the case that no laws have been broken, it's fair to say that the data sharing underpinning this discomfort is a violation of people’s reasonable expectation of privacy.

The scale of data collection and transfer using these mechanics is difficult to comprehend. Millions of web sites and apps have dozens of trackers installed. As a result, my behavioral data is collected by hundreds, perhaps thousands, of companies. Once data about my particular interests, activities and transactions is captured by entities that may or may not have a relationship with me, and have no particular loyalty to me, it’s totally out of my control.

The unfortunate by-product of a system like this is at the heart of the central privacy problem plaguing digital advertising. We can call this “the profiling problem.” In the model I’ve just described, ad platforms and advertisers have strong economic incentives to participate in this digital advertising system – and are disadvantaged compared to their competitors if they don’t participate. As a result of this system, ad platforms are able to build tremendously rich profiles about their user base including most of your browsing and buying behavior.

To be clear, I’m not calling out the ad platforms categorically for having bad motives. I believe there are many good actors in the ad tech ecosystem that understand the potential harms caused by the development of these profiles. The challenge is this: without clear rules (e.g. laws and regulations) ad tech companies are highly incentivized to gather and use data as aggressively as possible. Proactively eliminating the collection and use of third party data (e.g. pixel data) would put a platform at a massive disadvantage because ads that are data driven are just far more effective than those that are informed only by context or broad demographics. To address this incentive problem, we need to level the playing field by establishing clear criteria for what is and isn't acceptable.

Creating this level playing field requires a combination of efforts from legislators, regulators, advocates and technology companies. We believe there are three critical components that must come together to produce sustainable progress on digital privacy:

1) **Federal privacy legislation**, and supporting regulations, to provide baseline protections for all Americans and put an end to the race to the bottom in terms of data collection and use
2) **Strong enforcement authority** and action to make sure good actors aren't unduly disadvantaged when they take the initiative to improve their privacy practices
3) **Privacy enhancing technologies,** which, which will support massive advances in consumer privacy while ensuring advertising can continue to help businesses grow and keep content free

We've covered the importance of regulations and enforcement, given the incentives at play in the ad tech ecosystem, so now I'll focus on the technologies that can support a transition to a far more private approach to advertising.

**How Privacy Enhancing Technologies Work**

Privacy enhancing technologies (PETs) are a fairly broad class of technologies that enable confidential and private computing. PETs are used in many other industries and contexts. Financial services firms use them to collaboratively build fraud models without compromising individuals'' data by sharing it directly with other companies. Pharmaceutical companies use PETs to bring together disparate data sets to conduct clinical trials while ensuring no party has access to sensitive healthcare information.

The Census Bureau uses PETs to support research on census data without compromising individuals' privacy. In the context of advertising, PETs can be employed to support three key use cases:

- Measurement: Understanding how ads lead to outcomes like purchases
- Targeting: Serving ads to individuals likely to have specific characteristics or interests, such as runners, mothers of young children or university students
- Optimization: Improving the relevance and effectiveness of advertising by using algorithms to make ad delivery decisions in an automated manner

To support these use cases, one must match two sets of data, one from the ad platform with information about who saw the ads and the other from an advertiser with information about actions on the advertiser's site or app.

Historically, the advertiser information has been sent directly to the ad platform, which is what creates "the profiling problem" I discussed earlier. With a PET-based approach, however, the profiling problem can be nipped in the bud – instead of one party directly sharing data with the other, the data is processed by an intermediary that itself has no access to unencrypted data. All computation happens in a fully safe and encrypted environment.

Inside this secure system the two data sets are joined and computations take place – including measurement and correlations that create aggregated data and statistics (in the example above, an advertiser like Home Depot might learn that 4% of men my age who saw the ad ended up buying the product).

Importantly, however, after completing the computation and generating trusted aggregated results, the individual-level data used to generate those results is deleted. The aggregated results of these computations are then further anonymized by using privacy mechanisms such as Differential Privacy, which adds noise (effectively random data) to limit the likelihood that individuals can be re-identified using the aggregated results.

The aggregated and anonymized results are then shared with the advertiser and the ad platform. The end result is that everyone gets what they need, but no party has learned anything new about any individual. This is the promise of privacy enhancing technologies, and this is the model we have been building at Anonym.

**Summary**

In summary, we believe the notion that you cannot have both privacy and an efficient digital advertising ecosystem that support businesses of all sizes is a false dichotomy. We believe in a win-win set of solutions that includes (but is not limited to) the following:

- Increased protections for children and older minors beyond COPPA, which was enacted in an earlier era when the internet and its content was frequently analogized to television – hence the focus on age 13.
- A single federal statutory scheme that provides a baseline for how data is treated and that strongly limits or prohibits sharing of individual consumer data directly between companies.
- Unified protections that operate the same way in all states to provide protections to all Americans. We support ADPPA because it provides these unified consistent protections.
- Strong and clear enforcement authority for privacy regulators.
- Technology that guarantees privacy while still empowering businesses to operate efficiently, find customers and grow.
- Importantly, to keep incentives clean and encourage competition, these technology solutions should be open and transparent and operated by companies that do not sell data or advertising.

Bringing these critical elements together will be a powerful demonstration of how government, citizens, businesses, and advocates can work together to establish a law-driven, technology-backed baseline for data privacy protection. We believe this will provide a global roadmap for how regulation and technology can work hand in hand to respect people's fundamental right to privacy while enabling quality consumer experiences and supporting economic growth.

Thank you again, Chairman Bilirakis, Ranking Member Schakowsky, and the other honorable members of this committee for your time and attention. I look forward to answering any questions you may have about my testimony or about these issues generally.