



**Comments of the
Software & Information Industry Association (SIIA)
on the
Federal Trade Commission Hearings on Competition and
Consumer Protection in the 21st Century
August 20, 2018**

Topic #4: The intersection between privacy, big data and competition

About SIIA

With nearly 700 member companies, SIIA is the principal trade association of the software and digital content industries. Our members are global industry leaders in the development and marketing of software and electronic content for business, education, government and consumer markets. They range from start-up firms to some of the largest and most recognizable corporations in the world. SIIA member companies are leading providers of, among other things:

- Data analytics and artificial intelligence,
- business, enterprise and networking software,
- publishing, graphics, and photo editing tools,
- corporate database and data processing software,
- financial trading and investing services, news, and commodities,
- online legal information and legal research tools,
- education software, digital content and online education services,
- specialized business media,
- open source software, and
- many other products and services in the digital content industries.

Introduction

In providing our comments, we start first with identifying key goals. One goal is to ensure adequate privacy protection for U.S. citizens, whereby their personal information is protected from harm that could come from misuse of their data. Another goal is for U.S. policies to continue to promote a thriving internet and information-driven economy, where robust innovation drives strong economic growth, employing millions of Americans and providing transformative benefits for consumers. A third goal is to ensure that privacy protections are balanced in consideration of other important rights, such as free speech.

These goals are not mutually exclusive. Privacy policy and competition policy are covered by separate bodies of law. Privacy objectives should not be part of the objectives of competition policy. Still, public policy can establish a balanced framework providing for both strong privacy protection and thriving data-driven innovation. In order to strike this balance, privacy protections should be principles-based and focus on outcomes and consumer expectations, rather than complex consent procedures or prescriptive interface designs or formalistic documentation requirements. Focusing on procedures

companies must take over the outcomes they should achieve can be in tension with economic success and improving overall consumer protections, because companies get bogged down in the technicalities of compliance, rather than focusing on what is best for their community of users. But in fact, far from being in tension, well-calibrated privacy protections often contribute to economic success, improving consumer trust in specific brands, and the internet ecosystem overall.

A uniform, national approach to privacy protections will benefit consumers and spur innovation.

For many years, the United States has maintained an effective, if complex, regime to provide for strong data privacy and security protections for American’s sensitive information, including financial, health, student and children’s data. This risk-based regime consists of a series of sectoral laws targeting the concrete, specific harms that can arise from the misuse of information in contexts where sensitivity and privacy risks are heightened. This current regime—with FTC at its center—has the advantages of flexibility, a focus on harm, and strong regulation, rather than rigid check-the-box compliance procedures. This approach has balanced the goals of building and protecting consumer trust in online services, while also promoting innovation and economic growth.

The FTC, under its broad consumer protection mandate, enforces privacy protections by requiring companies to give people the information they need to make decisions about their data and by holding companies accountable for harmful uses of data. Congress has also developed sector- and information-specific privacy laws that require increased protections where information is collected by certain types of entities, such as health care providers, and for certain types of sensitive information, such as children's information. This combination of specific privacy laws and strong FTC enforcement provides robust privacy protections that are tailored to consumer expectations and potential harms.

Providing successful consumer privacy protections is a highly contextual task. FTC enforcement of privacy has therefore never been “one size fits all,” and it can never be. Companies take varying approaches to protect privacy, based on the circumstances involved, such as the nature of the data collected, the relationship between people and the company collecting that data, and people's expectations in a given context. Overall, the U.S. sectoral privacy regime is context-driven, as it is tailored to address privacy challenges presented by the collection and use of certain types of data.

This contrasts significantly with the recently implemented European General Data Protection Regulation (GDPR), which established a broad consent-based requirement for processing of virtually all data that pertains to consumers and extensive compliance processes that require substantial upfront and continuing expenditures. The exceptions from consent for processing based on legitimate interest have yet to be fully explored and might provide an important alternative to consent-based processing. The recently enacted California Consumer Privacy Act (CCPA) has many of the same structural and procedural flaws, although some of them derive not from considered judgment but from expedited drafting and a lack of legislative deliberation.

One of the concerns with both GDPR and CCPA is that they will create an overwhelming set of responsibilities for consumers to manage the collection and use of their data. As SIIA has highlighted in

past writing on big data and privacy, the notion of shifting responsibility for data protection to consumers is likely neither effective, nor desirable.¹

Policymakers, industry, and civil society must collectively assess the not only the impacts of the GDPR and CCPA, perhaps through the mechanism of a new privacy law that would establish a single, updated national approach.

There could be advantages in a new uniform privacy regime to solidify the current focus on sensitive practices and aligning the stringency of protective measures to consumer expectations and the risk of injury. It does not make sense to override or rewrite existing privacy laws that agencies including the FTC have implemented and interpreted for decades. But in areas not covered by a specific sectoral law, a uniform national policy might make sense. As we explore what such a standard would look like, it is important to understand and recognize the effectiveness of the FTC's privacy regime and to build on that tradition of a flexible, risk-based approach tied to the upcoming set of FTC hearings can play a significant role in helping to assess the status quo, and the potential need for new policies or regulations.

The FTC has been the chief federal agency on privacy policy and enforcement since the 1970s, when it began enforcing the Fair Credit Reporting Act, one of the first federal privacy laws, and one which relies less on consumer choice and more on other protective measures such as access.²

Looking forward, the FTC is well positioned to continue this data protection leadership in changing times, through strong law enforcement, policy initiatives, and consumer and business education.³

The ad-supported internet ecosystem has proven highly desirable and essential for businesses, consumers and the economy.

There is broad array of rich and diverse content available on the internet, including software, information and news content, video and music streaming services, interactive services such as email and social networks, have experienced robust growth over the last several years. As the internet ecosystem has expanded into what is known as the Internet of Things (IoT), where internet connectivity is ubiquitous across an increasingly wide range of electronic "smart" devices, digital content is increasingly provided across a diverse set of sites and apps and a wide-range of platforms, from computers, to tablets and smartphones, to televisions and video game consoles, to "wearable" and smart-home devices. This content is provided through various pricing models, ranging from flat-rate subscriptions, consumption-based pricing, to free ad-supported offerings.

As the internet-based media ecosystem has become richer and more diverse over more than two decades, one thing has remained constant: by far the most popular model among consumers is free, or low-cost ad-supported content. This conclusion is supported by significant data that captures the value consumers place on ad-supported content. Most notably, recent data from the survey research company Nielsen, finds that while the media landscape expands, the type of content consumers are

¹ SIIA, [Data-Driven Innovation, A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data](#) (September 2013).

² See FTC overview of consumer privacy resources: <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy>

³ See catalogue of recent data privacy enforcement actions, guidance and educational resources for businesses and consumers: <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises>

spending time with has remained fairly consistent. Ad-supported content remains the medium that consumers gravitate toward the majority of the time in their viewing habits.⁴ According to Nielsen data, the share of time spent with ad-supported content on platforms (such as TV, radio, smartphones, video games and tablets) for adults in 2017 was 86%—a number that has remained relatively flat over the past decade.⁵ The broad conclusion of this research is as follows:

Although consumption of ad-supported media has varied over the past 15 years, it is still far more dominant and successful than perception may indicate. Today, ad-supported content remains a consumption stalwart as consumers’ media palates expand and consumption habits swell. While such revenue models have existed for some time, they seemingly have the versatility and adaptability to keep pace with an ultimately dynamic and fragmented landscape. This new age of media consumption allows marketers and advertisers to reach consumers in more ways than ever before and do so with ease.⁶

The Network Advertising Initiative (NAI) recently conducted a consumer survey that produced similar results. In late 2017, NAI ran opinion polls and marketing research on internet users through a survey that obtained responses from 10,000 U.S. consumers to assess their opinions on privacy, digital advertising, and the ad-supported internet. The results revealed that consumers overwhelmingly prefer their online content to be paid for by advertising, at a rate of 67%, a result that was substantially consistent across all age-groups.⁷

Regarding privacy, the survey revealed that while 85% of respondents indicated that they were at least “somewhat concerned” about privacy on the internet, that the source of this concern varied widely, and that while the top privacy concerns were fear of data collection by hackers and governments entities, which combine for 72% of this fear, only 8% of users were most concerned about website and application publishers collecting data and 7% of users stated that data collection by advertising companies was their primary concern.⁸

While it is hard to estimate the overall value that advertising-based content provides to consumers, there have been multiple attempts to estimate or measure this. For instance, a survey commissioned by the Digital Advertising Alliance revealed that consumers valued ad-supported services, like news, weather, video content, and social media at \$99.77 per month, or \$1,197 a year. A large majority of surveyed consumers, 85%, stated they like the ad-supported model, and 75% indicated that they would greatly decrease their engagement with the Internet if a different model were to take its place.⁹

Other research has explored the value of different types of advertising. An economic study by Professors Howard Beales and Jeffrey Eisenach of Navigant Economics found that the use of cookie technology to increase relevance of advertising increased the average impression price paid by

⁴ Nielsen Company, [As the Media Universe Grows, Ad-Supported Content Remains a Preferred Source](#) (March 14, 2018).

⁵ Ibid.

⁶ Ibid.

⁷ [Digital advertising, online content, and privacy survey](#), Network Advertising Initiative (April 9, 2018).

⁸ Ibid.

⁹ [Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet](#), Commissioned by the Digital Advertising Alliance (May 2016).

advertisers by 60% to 200%, depending on a series of variables.¹⁰ This data underscores the value of interest-based advertising, whereby data used to determine relevance of the ads is a critical variable for successful ad-supported content.

Another critical way to look at the impact of ad-supported internet content is to measure the overall economic impact. A 2017 study by Harvard Business School Professor John Deighton found that the U.S. ad-supported internet created 10.4 million jobs in 2016. This research concluded that the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, which is double the 2012 figure, and accounts for 6% of U.S. gross domestic product.¹¹

Of course, this is not to suggest that ad-supported content is the *only* viable model, and that consumers are unwilling to pay for high-quality internet content. Indeed, subscriptions for many news publishers have recently experienced dramatic increases. For instance, the New York Times reported earlier this year that it added 157,000 net digital-only subscriptions in the fourth quarter of the year, pushing overall subscription revenue to more than \$1 billion for the year.¹² Other leading news publishers such as the Washington Post and the Wall Street Journal have also seen similar rises in subscriptions, particularly digital subscriptions.

It is worth noting that many of the areas where there is strong subscription growth, there is also a continually strong reliance on advertising revenue—this includes not only traditional news content providers, but also internet-based video content providers such as Roku, who recently reported that for the 6.7 billion hours streamed over Roku devices and Roku TVs in the first half of FY 2017, a full 43% were ad supported.¹³ In addition, Roku reported that 41% of its total revenue for that same period came from advertising.¹⁴

SIIA's member companies reflect the broad and diverse landscape of digital content, including both B2B and B2C services, small specialized providers and large industry leaders, providing and all types of content. A close look at SIIA members and other content providers reveals that producing high quality content and services and delivering this content to audiences across a diverse and ever-changing set of platforms is a costly business, one that requires scalable and sustainable revenue sources. In some cases, these content services are completely free and ad-supported. In others, they are provided through a combination of subscriptions and ad-support. The only significant category of purely subscription-based revenue is for certain specialized B2B content and services.

Looking forward, it is highly likely that internet content will continue to be provided similar to print media content and cable television service, where a mix of subscriptions and advertising models are essential to combine for the necessary revenue across a wide range of models to suit different consumers. There is little evidence that consumers would prefer to pay for internet content, rather than to receive interest-based advertising that make the content available for little or no cost. Overall, the ad-supported internet ecosystem has proven highly desirable and essential for businesses, consumers and the economy, and that this will remain true for the foreseeable future.

¹⁰ Beales, Howard , and Eisenach, Jeffrey, [An Empirical Analysis of the Value of Information Sharing in the Market for Online Content](#), commissioned by the Digital Advertising Alliance, January 2014.

¹¹ Deighton, John, [Economic Value of the Advertising-Supported Internet Ecosystem](#) (2017).

¹² Ember, Sydney, [New York Times Co. Subscription Revenue Surpassed \\$1 Billion in 2017](#), New York Times (February 8, 2018).

¹³ Wolk, Allan, [Ad-Supported OTT Isn't A Fad, It's The Future](#), Forbes (November 16, 2017).

¹⁴ Ibid.

Congress has created multiple statutory frameworks to specifically address circumstances that require increased privacy protections. The Commission should prioritize these areas for enforcement.

At the direction of Congress, the FTC is responsible for enforcing a wide range of privacy and data security statutes including the Fair Credit Reporting Act, the Do-Not-Call Implementation Act of 2003, the Children's Online Privacy Protection Act, the privacy and security provisions of the Gramm-Leach-Bliley Act (for nontraditional financial institutions), and the Fair and Accurate Credit Transactions Act of 2003. The Commission has also taken action against privacy and security practices that violate the prohibition on unfair or deceptive under Section 5 of the FTC Act.

Congress has repeatedly identified the need for increased privacy protections where information is collected by certain types of entities such as financial institutions and for certain types of sensitive information such as children's information. In addition to its general Section 5 authority, Congress has provided the Commission with specific regulatory and enforcement authority to ameliorate heightened risks in special contexts. The Commission should continue to prioritize its enforcement actions based on this type of assessment of risk.

The goal of antitrust enforcement should be consumer welfare.

The goal of antitrust policy should be what it has been for generations, namely, to make the market work better for consumers. In contrast, privacy policy aims to protect consumers from harm based on the collection, use and dissemination of personal information. They are distinct bodies of law and should proceed in relative independence from each other. Antitrust policy moved away from its original goal of curbing the economic and political power of large corporations in the 1930s when President Franklin Roosevelt's antitrust chief, Thurmond Arnold, established the goal of consumer welfare as the paramount objective, rather than focusing on firm size.

University of California professor Carl Shapiro, recently restated this goal as: "protecting the competitive process so consumers receive the full benefits of vigorous competition." Through the ups and downs of enforcement styles in the ensuing period, this objective has been the constant lodestar of antitrust and has been repeatedly upheld by the Courts.¹⁵

FTC Chairman, Joseph Simons, clearly articulated earlier this year without qualification: "The FTC is all about protecting and improving consumer welfare."¹⁶

There is a real need for vigorous antitrust policy, because the marketplace might not automatically deliver an abundant supply of low-price, high-quality products and services. Antitrust policy should seek to maintain and foster competition so as to lower price, improve quality, and increase the output of products and services. Conversely, it should avoid measures that harm consumers by raising prices above competitive levels or by denying them services or features that they value.

Many commentators are concerned about broader public policy issues and want to enlist antitrust as a policy lever to advance reforms in these areas. Among these goals are better wages for workers, greater

¹⁵ Shapiro, Carl, [Antitrust in a Time of Populism](#) (Oct. 24, 2017).

¹⁶ [Statement of Joseph Simons](#), Nominee, Federal Trade Commission (February 14, 2018).

equality in the distribution of income and wealth, and constraints on the ability of large organizations to influence the outcomes of public policy debates. Some want antitrust law to reform what they perceive as unjust business models in the credit card industry, or even to address the problem of fake news.

These issues are important, perhaps equally or more important than promoting competition, because they go to the question of the strength and legitimacy of our democratic political processes. But they should not be addressed by antitrust authorities and courts.

As Carl Shapiro says, “the corrupting power of money in politics...is far better addressed through campaign finance reform and anti-corruption rules than by antitrust.” As for income inequality, “other public policies are far superior for this purpose. Tax policy, government programs such as Medicaid, disability insurance, and Social Security, and a whole range of policies relating to education and training spring immediately to mind.”¹⁷

Moreover, as law scholar Herbert Hovenkamp has found, the larger goals that antitrust might foster, “often operate at cross purposes with one another. For example, to the extent that large firms are more efficient, their output will be higher, and they will provide more jobs. Further, large firms historically pay substantially higher wages and salaries than smaller firms.” Do we really want to break up large firms if the result is lower wages for workers?¹⁸

Vigorous antitrust enforcement should target price increases and declines in the quality and output of goods and services created by failures of the competitive process. Companies should not be allowed to take advantage of their market position to harm the consumer interest in low-price, high-quality goods and services. Antitrust officials including the FTC should keep their eye on the consumer welfare ball, rather than trying to remedy real or perceived problems that are outside the scope of their knowledge and expertise.

Data is not a barrier to entry in the Internet ecosystem.

There is no question that data is a vital asset in the 21st Century digital economy, but it has also proven to be plentiful. Unlike the natural resources that drove previous industrial revolutions, data is not a finite commodity that one entity can obtain and prevent others from obtaining. Data available from one online source, for instance, is usually available from other sources. People who use one social network, also use others. They are likely to have accounts with more than one of Facebook, Pinterest, Snapchat, YouTube, LinkedIn, and Twitter, all of which collect the user data they need deliver a compelling service to consumers. The Pew Institute recently found that the typical American uses three of these major social media platforms.¹⁹ People don’t keep economically valuable data a secret from these other platforms and there is nothing one platform can do to stop them from engaging with others elsewhere.

¹⁷ Shapiro, Carl, [Antitrust in a Time of Populism](#) (Oct. 24, 2017).

¹⁸ Hovenkamp, Herbert, [Whatever Did Happen to the Antitrust Movement?](#) (February 10, 2018). Notre Dame Law Review.

¹⁹ Smith, Aaron, Anderson, Monica, [Social Media Use in 2018](#), Pew Research Center (March 1, 2018).

Moreover, as MIT business professors Brynjofsson and McAfee note, small data sets are often good enough to provide the insights needed to power a business.²⁰ In particular, they note that “you may not need all that much data to start making productive use of machine learning” and “sufficient data is often surprisingly easy to obtain.”²¹

In the data economy, the question isn’t whether data is valuable but whether there’s enough good data available for competitors to use. When competition authorities have faced this context-dependent factual question in recent years in specific merger cases, time after time they determined that competitors would have post-merger access to enough data.²²

Tensions exist between competition policy and privacy.

To fix competitive problems in the tech industry, some commentators are urging greater privacy regulation. For instance, The Economist has urged regulators to give people “more control over their information” as a way to tame tech.²³

In fact, this has been an objective of data protection policy on both sides of the Atlantic for over a generation. The EU just finished a far-reaching update of its privacy law, the General Data Protection Regulation, went into effect in May 2018. This is the most sweeping reform of data protection laws in history. To comply, technology companies and other affected businesses will be updating their systems for years to come. The California privacy law also aims at providing this additional control.

But this privacy measure would hurt all competitors, not promote competition. What The Economist seems to mean, however, is not that we should protect user privacy, but that we should use privacy law to dry up the supply of data to tech companies. It is hard to see how this furthers competition. Instead, the lack of data would hurt everyone in the market.

The Economist suggests a further, and contradictory, data reform – user data should be turned over to anyone willing to pay a compulsory license fee. As Barry Nigro, the Deputy Assistant Attorney General for Antitrust for the U.S. Department of Justice noted recently, this forced sharing of a company’s critical asset would tend to dry up the incentive to invest in innovation.²⁴ And there is no need for this step. As pointed out above, competition authorities have repeatedly found that data needed for competitors to challenge incumbents is in plentiful supply.

But more important from the point of view of the intersection of privacy and competition, which is the focus of the Commission’s inquiry, compulsory data sharing is hard to reconcile with the privacy rights of data subjects. Under mandated data sharing all competitors in the same market would have access to the same consumer information in order to create an equal competitive playing field. As a result,

²⁰ Harvard Business Review, [The Business of Artificial Intelligence](#) (July 2017).

²¹ Ibid.

²² See the summary of recent cases in Marc Bourreau, et al., Big Data and Competition, CERRE, 2017, p. 30-31 available at http://cerre.eu/sites/cerre/files/170216_CERRE_CompData_FinalReport.pdf

²³ The Economist, [Competition in the digital age: How to tame the tech titans](#) (January 18, 2018).

²⁴ Deputy Assistant Attorney General Barry Nigro Delivers Remarks at The Capitol Forum and CQ’s Fourth Annual Tech, Media & Telecom Competition Conference (December 13, 2017). <https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-barry-nigro-delivers-remarks-capitol-forum-and-cqs>

information that a user shares with one company would then be automatically available to the entire marketplace. This appears to be a direct threat to consumer privacy.

In addition, new privacy regulations could entrench established companies in their current market position by imposing additional compliance costs on everyone. These compliance costs can themselves create competitive entry barriers. Commissioner Noah Phillips recently expressed this concern, noting, “laws and regulations intended to promote privacy may build protective moats around large companies (some of which already possess significant amounts of data about people) by making it more difficult for smaller companies to grow, for new companies to enter the market, and for innovation to occur—and insist that competition be part of our conversation about privacy.”²⁵

Adam Thierer also recently reached the conclusion that new regulations aimed at curbing the privacy practices of existing tech platforms, but imposed on all companies, will likely “end up hurting smaller rivals more and create barriers to new entry and innovation going forward.”²⁶ U.S. Department of Justice Antitrust Division lead, Makan Delrahim, has made a similar point, noting that the costs of regulatory schemes “create entry barriers” that incumbents might be willing to incur “if the same cost is applied to new competitors.”²⁷

Of course, this is not an argument against needed privacy protections if they are truly needed. Rather, policymakers need to be mindful that any new regulatory policies come with additional costs and make sure that the gains from these new regulations are commensurate with these additional costs, including the potential cost to competitive entry.

²⁵ Phillips, Noah, [Keep It: Maintaining Competition in the Privacy Debate](#) (July 27, 2018).

²⁶ Thierer, Adam, [The Week Facebook Became a Regulated Monopoly \(and Achieved Its Greatest Victory in the Process\)](#).

²⁷ Assistant Attorney General Makan Delrahim Delivers Keynote Address at the University of Chicago's Antitrust and Competition Conference (April 19, 2018). <https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-keynote-address-university-chicagos>