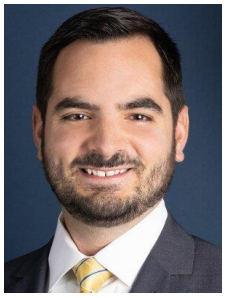
Antitrust Law As A Tool Against Privacy Abuses

By **William Reiss and Matthew Geyer** (May 5, 2022)

William Reiss



Matthew Geyer

Typically, when one thinks of anti-competitive harm, one envisions a consumer or business paying an inflated price for a product or service resulting from an unlawful monopoly or agreement among competitors.

And, in most antitrust cases, that is the very landscape. But as social media and technology continue to expand into new frontiers by offering free products and services to users; commentators, regulators, and perhaps most importantly courts have begun to recognize a new concept of anti-competitive harm: harm to privacy.

As the biggest players in the Big Tech and social media space continue to expand their power and dominate their respective markets, users have suffered significant encroachments to their privacy as these tech behemoths have effectively mined their personal data. The mining of consumer data by these big players has arguably enabled them to maintain their dominant positions in their respective markets, further deterring competition and harming consumers as a result.

Of course, the drafters of the Sherman and Clayton Antitrust Acts could not have anticipated the convergence of privacy law and antitrust law at the time these statutes were passed, well over 100 years ago. But with the advent and rapid acceleration of technology and social media in the 21st century, the debate has become unavoidable with regulators and lawmakers looking for ways to rein in the power of Big Tech, particularly through federal legislation.

And while the debate over privacy's role in antitrust law has been brewing among scholars, commentators and government officials for over a decade, courts have not uniformly recognized harm to privacy as an anti-competitive harm or, relatedly, that the antitrust laws should be used as a tool to combat privacy violations.

This article explores that debate and how the courts have reached varied outcomes — with potentially momentous effects — when analyzing privacy issues through an antitrust lens.

Privacy as Anti-Competitive Harm Enters the U.S. Legal Landscape

The Federal Trade Commission's former Commissioner Pamela Jones Harbour's December 2007 dissenting opinion in the FTC's approval of Google Inc.'s acquisition of DoubleClick Inc. is widely recognized as the first time a U.S. regulator or court expressed a view that harm to privacy could constitute an anti-competitive harm and that the antitrust laws were the proper enforcement mechanism.

In her DoubleClick dissent, Harbour argued that the FTC's majority opinion approving the merger and closing its investigation failed to "adequately address" either "the competition [or] privacy interests of consumers."[1] Harbour asserted that a "broader approach" to the competitive analysis was necessary since the merger "combine[d] not only the two firms' products and services, but also their vast troves of data about consumer behavior on the Internet."[2]

Given the extensive amount of consumer data at issue, Harbour opined that the merger reflected an "interplay between traditional competition and consumer protection issues," putting the FTC in a "unique position" to evaluate the implications of the merger from both a competition and consumer protection perspective.[3]

Harbour's more expansive view of antitrust law's role in regulating privacy abuses gained traction in the immediate aftermath of her dissent. For example, in a subsequent unrelated FTC investigation against Google addressing allegations that Google unfairly promoted its own search content while demoting competitors' content, then-Commissioner Thomas Rosch hinted in his concurrence and dissent that Google's hoarding of consumer data may have been done not solely for consumer benefit, but also to maintain Google's "monopoly or near monopoly position."[4]

Other FTC commissioners have followed suit. Commissioner Rebecca Slaughter stated in 2019 that privacy can be viewed as both a metric of product quality and an element of consumer harm,[5] and former Commissioner Rohit Chopra has opined that increased data collection is "akin to price increases" and should be analyzed as such in antitrust cases.[6] The Biden administration has also entered into the debate, declaring that "unfair data collection and surveillance practices [] may damage competition, consumer autonomy, and consumer privacy."[7]

Scholars have echoed these sentiments, noting that the costs associated with inadequate privacy may actually degrade consumer welfare more than artificially high prices.[8] Specifically, these scholars argue that consumers, companies and the government end up paying billions of dollars each year to redress identity theft and data breaches due to lack of privacy controls associated with the consumer data collected by the major "Big Tech" players.[9]

Scholars further argue that antitrust laws should be used to condemn the practices leading to such inadequate privacy protections.[10]

Furthermore, in recent remarks to the International Association of Privacy Professionals' Global Privacy Summit in Washington, D.C., FTC Chair Lina Khan signaled that the FTC is working to take an "interdisciplinary approach" to enforcement by looking at data practices and related privacy issues through both a consumer protection and competition lens "given the intersecting ways in which wide-scale data collection and commercial surveillance practices can facilitate violations [of consumer protection and competition laws]."[11]

This official shift in approach is notable, as government enforcers and private plaintiffs have traditionally sought to prosecute privacy violations through consumer protection statutes. However, as Khan's remarks seem to imply, relying solely on consumer protection statutes has proven insufficient, leading courts and regulators to look to competition law as a more robust and effective tool in prosecuting privacy violations.

Criticisms of Viewing Privacy Through an Antitrust Lens

While the notion that the antitrust laws should be used as a tool to combat privacy violations has garnered growing acceptance, it is not without its critics. Some current and former FTC commissioners have argued that viewing privacy issues through an antitrust lens is misguided because competition law and privacy law "have different aims, and use different tools to achieve those aims," such that conflating the two may lead to "incoherence, and even contribute to the erosion of the rule of law," FTC Commissioner Noah J. Philips said in 2020.[12]

Others have stated that future antitrust rulings limiting the ability of a company to collect and analyze consumer data may run into First Amendment issues because such restrictions may inhibit the free flow of commercial information and thus, "impede[] the ability of advertisers to convey their commercial messages to consumers," said James C. Cooper, a former FTC official.[13]

Scholars have also argued that consumers may actually benefit from the data mining practices of companies in the form of improved services and quality of content, such that potential benefits outweigh any potential privacy harms.[14] Specifically, the more data a company can mine from consumers, the more insight it will have into consumer preferences, allowing it to improve the quality of its content and to sell more finely targeted ads to consumers.[15]

Similarly, some commentators worry that enhancing privacy protection at the expense of preventing data mining may even cause companies to start charging for the use of otherwise free services, as a lack of consumer data may lead to a lack of targeted advertising and thus, loss of advertising revenue.[16]

The Courts Weigh In

The courts have also recently waded into the debate, as highlighted by two recent cases that analyzed privacy issues through an anti-competitive lens but in two different contexts. In the 2021 Epic Games Inc. v. Apple Inc. decision, the U.S. District Court for the Northern District of California considered benefits to privacy as a pro-competitive justification to otherwise potentially anti-competitive conduct.[17]

Epic Games alleged that Apple's App store restrictions — including a prohibition against the distribution of iOS apps through alternative app stores and the mandatory use of Apple's In-App Purchase payment system — were anti-competitive and foreclosed competition in the market for global gaming transactions.[18]

Apple argued that its restrictions had pro-competitive justifications — namely, that the restrictions help to strengthen privacy and security protections for users.[19] In ultimately ruling for Apple after a bench trial, the court agreed that while Apple's restrictions did indeed produce anti-competitive effects, Apple's actions were shielded by its pro-competitive security justifications.

Specifically, the court held that compliance with its restrictions required "human review," and this review helps "to protect security by preventing social engineering attacks" and "protects against fraud [and] privacy intrusion."[20] Thus, Apple had effectively used enhanced privacy as a "shield" against allegations of anti-competitive conduct.

In a different context, the U.S. District Court for the District of Columbia also analyzed privacy issues through a competition lens and concluded that harm to privacy may constitute an anti-competitive harm that can be addressed by the antitrust laws. In Federal Trade Commission v. Facebook Inc.[21] the FTC brought allegations against social media giant Facebook, now Meta Platforms Inc., for unlawful monopoly maintenance under Section 2 of the Sherman Act.[22]

Specifically, the FTC alleged in its amended complaint that Facebook willfully maintained its monopoly power in the personal social networking services, or PSN, market through its anti-competitive acquisitions of nascent competitors WhatsApp and Instagram and by

maintaining and enforcing anti-competitive agreements to deter competitive threats to its monopoly.[23]

The FTC further alleged that Facebook's anti-competitive conduct harmed the "competitive process" by decreasing, among other things, privacy and data protections available to consumers in the PSN market.[24]

With respect to anti-competitive harm, Facebook argued in its motion to dismiss that the FTC could not allege harm in the "archetypal form of increased consumer prices," since Facebook, Instagram and WhatsApp are all provided to consumers free of charge.[25]

While the court agreed, it also acknowledged that the FTC sufficiently pled "harm to the competitive process and thereby harm [to] consumers."[26] In denying Facebook's motion to dismiss the amended complaint, the court noted that the FTC identified "a host of other harms" to the competitive process — and thus, to consumers in the PSN market — including a "decrease in service quality, lack of innovation, decreased privacy and data protection, excessive advertisements and decreased choice and control with regard to ads, and a general lack of consumer choice in the market for such services."[27]

The court further held that the FTC adequately alleged that the lack of meaningful competition in the PSN market at the hands of Facebook's monopolistic conduct has allowed Facebook to "provide lower levels of service quality on privacy and data protection than it would have to provide in a competitive market."[28]

The court also highlighted concrete examples of how Facebook has diminished privacy offerings to its consumers through its acquisitions of WhatsApp and Instagram. For example, prior to the acquisitions, WhatsApp had heavily invested and embraced "privacy-focused offerings and design," all of which were alleged by the FTC to have lessened and scaled backed after Facebook's acquisition.[29]

The court observed that Facebook likely would not have been able to scale back these protections in a competitive market, as there is an "intuitive notion" that consumers value and may even prefer increased privacy protections.[30] This observation, the court explained, is buttressed by the "advent of federal legislation addressing various privacy and advertising concerns related to consumer technology" that have come to light in the last few years.[31]

A New Path Forward?

The court's decision in Facebook is particularly notable because while it is not the first time a court has analyzed privacy issues through a competition lens, it appears to be the first time a court has recognized "decreased privacy and data protection" for consumers as a form of anti-competitive harm.

In so doing, the court may have begun to formally bridge the gap between privacy and antitrust law, opening the door for similar suits to be filed in the future. The Facebook decision is consistent with the enforcement agenda set forth by regulators and President Joe Biden.

Given these facts, it seems highly likely that additional antitrust cases seeking redress for privacy harms will be brought by both government and private actors. How these cases play out will serve a critical role in reshaping antitrust jurisprudence. As antitrust is having its moment in the sun, the time seems ripe for these changing frontiers to materialize.

William V. Reiss is a partner and Matthew J. Geyer is an associate at Robin Kaplan LLP.

[1] Dissenting Statement of Commissioner Harbour at 1, In the matter of Google/DoubleClick, F.T.C. File No. 071-0170 (Dec. 20, 2007), https://www.ftc.gov/sites/default/files/documents/public_statements/" target="_blank" rel="noopener noreferrer">https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf.

[2] Id. at 4.

[3] Id.

[4] Concurring and Dissenting Statement of Commissioner Rosch at 1 n.1, In the matter of Google, Inc., F.T.C. File No. 111-0163 (Jan. 3, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/concurring-and-dissenting-statement-commissioner-j.thomas-rosch-regarding-googles-search-practices/130103googlesearchstmt.pdf.

[5] Colin Kass et al., The Privacy and Antitrust Paradox in the Age of Data, Anti-Corruption Report at 2 (Feb. 16, 2022), https://www.jdsupra.com/legalnews/the-privacy-and-antitrust-paradox-in-7828628/.

[6] Id.

[7] Biden Administration, Executive Order on Promoting Competition in the American Economy at § 5(h)(i) (July 9, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.

[8] Gregory Day & Abbey Stemler, Infracompetitive Privacy, 105 Iowa L. Rev. 61, 61 (2019).

[9] Id. at 64.

[10] Id. at 66.

[11] Allison Grande, FTC Exploring Ways To Revamp Privacy Approach, Chair Says, Law360 (Apr. 11, 2022), https://www.law360.com/articles/1482944/ftc-exploring-ways-to-revamp-privacy-approach-chair-says.

[12] Noah J. Phillips (FTC), Should We Block This Merger? Some Thoughts on Converging Antitrust and Privacy, The Center for Internet and Society at 2 (Jan. 30, 2020), https://cdn.lawreportgroup.com/acuris/files/. anti-corruption-report/phillips_-_stanford_speech_10-30-20.pdf; see also Kass, supra note 5 at 2.

[13] James C. Cooper, Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity, 20 Geo. Mason L. Rev. 1129, 1138–43, 1140 (2013).

[14] Id. at 1135-36.

[15] Id.

[16] Kass, supra note 5 at 3.

[17] No. 4:20-CV-05640-YGR, 2021 WL 4128925 (N.D. Cal. Sept. 10, 2021).

[18] Id. at *3.

[19] Id. at *70.

[20] Id. at *101-02.

[21] No. CV 20-3590 (JEB), 2022 WL 103308 (D.D.C. Jan. 11, 2022).

[22] 48 State Attorneys General have brought a similar case against Facebook in the D.C. District Court. See State of New York, et al. v. Facebook, Inc., No. 1:20-cv-03589 (D.D.C.).

[23] These alleged "anticompetitive agreements" included Facebook polices that prohibited third-party, freestanding apps from accessing Facebook's API if those third parties competed with Facebook.

[24] Id. at *12-13.

[25] Id. at *12.

[26] Id.

[27] Id. at *13.

[28] Id.

[29] Id.

[30] Id.

[31] Id.