Anti-Corruption Report
An Acuris company

anti-corruption.com

February 16, 2022

DATA PRIVACY

The Privacy and Antitrust Paradox in the Age of Data

By Colin Kass, Ryan Blaney, David Munkittrick and Kelly Landers Hawthorne, *Proskauer*

It used to be privacy was largely the domain of constitutional law and patient health care law: the Fourth Amendment, and then the Fourteenth Amendment, and the Health Insurance Portability and Accountability Act (HIPAA). Today, privacy is the practice of navigating the state-by-state patchwork of data security laws and regulations, subject matter specific privacy laws, and a number of federal rules stuck in there for good measure. Dealing with health-related information? Look to HIPAA. Biometric information? Illinois has a law for that. Financial information? Look to the Gramm-Leach-Bliley Act (GLBA). Antitrust, of course, has lumbered along for over one-and-a-quarter centuries based largely on two federal statutes. At first blush, antitrust and privacy would seemingly have little to do with one another, each content to operate in their respective spheres.

Yet, over the last few years, those spheres have steadily inched closer together to the point where now, they are like two tectonic plates grinding together, sending out ripples across the legal landscape. Data has brought them together. And data is everywhere. By some measures, internet users generate something in the order of 2.5 quintillion bytes of data every day. Data drives industries, economies, and competition. And with data, particularly personal data, comes cybersecurity and data security and privacy issues (we use cybersecurity, data security and privacy here interchangeably). While modern antitrust practice certainly utilizes data (think economists and their regressions), it does not yet quite know how or whether to treat data privacy or data security as an element of competition.

Sometimes privacy can be a procompetitive rationale for defendants to wield in the face of accusations of anticompetitive conduct, while at others, plaintiffs and regulators are starting to target privacy practices and misleading privacy disclosures and representations themselves as potentially anticompetitive. And the ground rumbles.

This article attempts to make some sense of the current state of data security and privacy in antitrust by first peering briefly to the past. In the end, data privacy may be like price discrimination, or bundling. Everyone does it (collects and uses data), and the vast majority of the time, it benefits competition. The question, of course, is when might it do the opposite? While *increased* data privacy practices will in most cases be procompetitive, antitrust is generally not in the business of determining how much privacy is enough privacy, just as antitrust is not in the business of telling companies how hard they should

compete, or for which customers. Thus, to borrow from duty-to-deal jurisprudence, privacy may be "at or near the outer boundary" of antitrust liability.

See "How Do You Put a System of Privacy and Security Controls in Place When Your Target Keeps Moving?" (May 26, 2021).

Privacy Gradually Enters the Antitrust Lexicon

One of the first acknowledgements that data security and privacy may have competitive effects was in a December 2007 dissenting opinion to the FTC's approval of Google's acquisition of web advertiser DoubleClick. Commissioner Pamela Jones Harbour predicted that "the combination of Google and DoubleClick [had] the potential to profoundly alter the 21 century internet-based economy – in ways we can imagine, and in ways we cannot," and argued that the FTC's approval of the merger did not "adequately address[]" either competition or privacy interests. Specifically, Commissioner Harbor noted that the "transaction will combine not only the two firms' products and services, but also their vast troves of data about consumer behavior on the internet.

Thus, the transaction reflects an interplay between traditional competition and consumer protection issues." Commissioner Harbour would have addressed "the privacy issues as part of [the FTC's] analysis of the transaction" because, she argued, "[t]raditional competition analysis . . . fails to capture the interests of all the relevant parties." The majority did not consider the effect of the combined firm's data collection on the consumers whose data are at issue given that the consumers do not have a business relationship with Google or DoubleClick (advertisers do).

See "Privilege, Data Privacy and Human Resources in Cross-Border Investigations" (Oct. 31, 2018).

From Dissent to Mainstream

Much has changed since Commissioner Harbour's 2007 dissenting opinion. Other Commissioners have joined the chorus suggesting antitrust enforcement can be used to advance privacy protections, and the view has arguably moved from the dissent to mainstream. In November 2019, Commissioner Rebecca Slaughter stated that privacy can be viewed as a metric of product quality and an element of consumer harm. Similarly, Commissioner Rohit Chopra said that increased data collection is "akin to price increases," and should be treated as such in antitrust analysis. The prior Assistant Attorney General for Antitrust, Makan Delrahim, said, "Privacy, for example can be an important dimension of quality, and so by protecting competition, we can have an impact on privacy and data protection." And last year, President Biden's executive order called "unfair data collection" a persistent and recurring practice[] that inhibit[s] competition."

Not everyone agrees. Commissioner Noah Phillips has made clear he believes viewing privacy through an antitrust lens is misguided. While one might evaluate privacy as "a qualitative parameter of competition," "competition law is not designed to protect privacy," he has argued. "[A]ddressing [privacy and competition law] together will lead to incoherence, and even contribution to the erosion of the rule of law."

A Proxy for Price?

This is all subject to debate, of course, and underlies one of the questions posed in the agencies' request for public comment on a potential overhaul of the merger guidelines: "Can 'quality' and other characteristics play the same role as price in market definition?" While the current merger guidelines recognize that "enhanced market power can also be manifested in non-price terms and conditions that adversely affect customers, including reduced product…," increased data collection may actually improve other aspects of product quality (such as performance of algorithms). One could argue consumers do not participate on social media platforms or e-commerce sites seeking out privacy. Indeed, perhaps quite the opposite. When it comes to market definition, the only accepted tests today focus exclusively on price: the Small but Significant Non-Transitory Increase in Price (SSNIP).

While there are subjective aspects to price – one person's trash is another's treasure – everyone agrees paying a lower price for the same thing is better than paying a higher price. That does not translate to privacy so easily. Increased privacy may come at the expense of other metrics, including price, or even competition itself. Zero price platforms are fueled by advertising dollars, which are fueled by user data. If the data goes away, zero prices may as well. This is one of the primary arguments posed against the new tech-focused legislation pending in Congress: that forced competition will harm privacy. And this creates a dialectic in which privacy may at once be a procompetitive benefit and inhibit competition.

See "Balancing Legalese and Simplicity in Modern Privacy Policies" (Oct. 27, 2021).

Sword or Shield? Privacy in Antitrust Litigation

Privacy as Procompetitive

This tension is playing out in litigation as well as legislation. Last year, Apple scored a trial victory against Epic Games, wielding privacy as procompetitive justification. Epic alleged that Apple's App Store restrictions violated federal and California antitrust laws. As a condition for obtaining a license to design and distribute apps on Apple mobile devices, all app developers must enter into Apple's Developer Program License Agreement and abide by the App Store Review Guidelines. The Agreement prohibits the distribution of iOS apps through alternative app stores and mandates the use of Apple's In-App Purchase (IAP) payment system for all purchases of digital content to be consumed within an iOS app. Apple argued that its prohibitions "help[] ensure[] a safe and secure ecosystem. This benefits both users, who enjoy stronger security and privacy, and developers, who benefit from a larger audience drawn by these features."

The court recognized that Apple's prohibitions have some anticompetitive effects because they foreclose competition from other stores and reduce innovation in game distribution services. Nonetheless, the court accepted Apple's security justification. "[C]entralized app distribution enables Apple to conduct app review, which includes both technical and human components." Human review "provides a safe and trusted user experience on iOS, which encourages both users and developers to transact freely and is mutually beneficial."

Privacy as Anticompetitive

On the flip side, Texas and 14 other states and territories have sued Alphabet, challenging, among other things, their plan to eliminate third-party cookies from its Chrome browser, which the states claim almost all non-Alphabet publishers use to track users and target ads. Removing cookies, of course, enhances privacy, but the States argue this harms competition because advertisers rely on the cookies for targeted ads.

So which one is it? Are enhanced privacy protections procompetitive, or do they harm competition?

Challenging Changes to Privacy Policies

There does not appear to be meaningful dispute over the first question – that privacy protection can be a legitimate and pro-competitive goal – so we focus on the second. Can a change in privacy practices or privacy disclosures to consumers implicate the antitrust laws, and if so, when?

Let's assume the predicate hurdles are cleared: the defendant has monopoly power in a relevant market (each, of course, has its own set of significant issues). And let's assume our defendant operates an online marketplace. It changed its privacy practices to limit the data third-party sellers can collect and access about consumers in the marketplace. What is that if not a refusal to deal on particular terms? As the Supreme Court confirmed in its 2004 *Trinko* decision:

> Firms may acquire monopoly power by establishing an infrastructure that renders them uniquely suited to serve their customers. Compelling such firms to share the source of their advantage is in some tension with the underlying purpose of the antitrust law, since it may lessen the incentive for the monopolist, the rival, or both to invest in those economically beneficial facilities.

As such, courts are "very cautious in recognizing [] exceptions" to a firm's right to choose its business partners "because of the uncertain virtue of forced sharing." *And* judges are generally loath to impose particular terms on parties' business dealings.

A challenge to changed privacy practices under Section 2 of the Sherman Act must navigate the "narrow-eyed needle" of *Aspen Skiing* – a case "at or near the outer boundary" of antitrust law. In *Aspen Skiing*, the court imposed a duty to deal where a course of dealing arose in a competitive market and was later terminated after the defendant acquired monopoly power. That is a high bar, and rightfully so.

Consider the impact of our defendant's actions. An online platform competes on several levels: to attract consumers; to attract merchants; to attract advertisers, and, potentially, in the collection of user data consistent with its privacy notices and disclosures. If our defendant restricts access to data or adds new consumer privacy rights (such as the right to opt out of marketing or the right to delete their personal information) it is generally a win for privacy. But it may harm merchants or advertisers operating on the platform who had utilized that data or formed entire business models around the data. Yet generally, antitrust should leave that privacy win alone unless the *Aspen Skiing* indications are present. And that is one of the arguments made in Alphabet's recent motion

to dismiss the state AGs' complaint. Still, there remain potential paths available to plaintiffs to circumnavigate the *Aspen Skiing* restrictions, such as if the plaintiff can show the privacy justifications are pretextual.

Now, let's assume our defendant, instead of increasing its data privacy practices, decreased them, and allowed for greater data collection and sharing among third-party sellers and advertisers on its marketplace. Even assuming data privacy can be conceived of and treated like a price paid by consumers, the antitrust laws should have little to say, for "the Sherman Act imposes no duty on firms to compete vigorously, or for that matter at all, in price."[1] And increased data may lead to increased competition among the merchants and advertisers on the platform. If the choice to lower privacy practices is not well-taken by consumers, they will simply go elsewhere.

See "How to Facilitate a Safe and Privacy Compliant Return to Work: Policies and Protocols" (May 27, 2020).

Data Privacy Is Here to Stay as an Antitrust Issue

All this is not to say companies may sally forth with whatever data privacy practice they wish without regard to the antitrust laws. Quite the opposite. If anything, there is more scrutiny today on data practices than ever before, under both competition and consumer protection regimes, and particularly regarding the impact of data aggregation on emerging companies' ability to compete. Data privacy may be a good defense in litigation, and *Trinko* may provide some protection for changes to privacy practices that might impact competitors, but companies can expect these issues to arise with increasing frequency in both litigation and merger investigations, where the agencies have more discretion.

As litigations continue to wind their way through the courts, things to watch out for in the near term include the FTC's push to exercise its rulemaking authority for the first time in decades, and the potential overhaul of the merger guidelines. Biden's executive order encouraged the FTC to consider rulemaking to address "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy," and it appears the FTC may be poised to act on that suggestion. The DOJ and the FTC recently issued a request for public comment on potential changes to the merger guidelines, which could include exploring ways to define relevant markets based on factors like privacy rather than price. It asks, for example, "Does the focus on the SSNIP test in implementing the Hypothetical Monopolist Test specifically, and in undertaking market definition more broadly, obscure the various types of harms in addition to price effects that may arise?"

Because data has in many ways become the currency of competition, data privacy and antitrust issues will inevitably intertwine, and as we've seen, may often pull in opposite directions. And so we must aspire to F. Scott Fitzgerald's ideal: "to hold two opposed ideas in mind at the same time and still retain the ability to function." To recognize the spheres of antitrust and privacy as separate, but also that they will overlap in both complementary and contradictory ways.

Colin Kass is a partner in Proskauer's litigation department and co-head of the firm's antitrust group. As a seasoned trial lawyer, he advises a wide range of industries, including financial services, health care, sports, media, pharmaceuticals and automotive markets, and spans the full-range of antitrust and unfair competition-related litigation, including class actions, competitor suits, dealer/distributor termination suits, price discrimination cases, criminal price-fixing probes and merger injunctions.

Ryan Blaney is the head of Proskauer's global privacy & cybersecurity group and a partner in the firm's health care practice and advises on regulatory compliance, enforcement, litigation, investigations and transactions in the areas of data privacy, cybersecurity, health care and emerging technologies. His clients include private equity firms, asset managers, and companies in the health care, life sciences, retail and technology industries.

David Munkittrick is senior counsel at Proskauer and focuses his practice on complex and large-scale antitrust, copyright and entertainment matters in all forms of dispute resolution and litigation, from complaint through appeal. He has been involved in some of the most significant antitrust matters over the past few years, obtaining favorable results for Fortune 500 companies and other clients in bench and jury trials involving price discrimination and group boycott claims.

Kelly Landers Hawthorne is an associate in Proskauer's litigation department and a member of the firm's antitrust and product liability groups. She counsels clients in litigations and due diligence across a range of industries, including consumer products, life sciences, health care, education, hospitality, sports and entertainment.

Brooke Gottlieb, a former associate at Proskauer, also contributed to this article.

---

[1] *In re Text Messaging Antitrust Litig.* Collusion on data privacy policies may be a different question, but such policies are generally publicly available in a website's terms and conditions and so could not form the basis of an unlawful conspiracy.