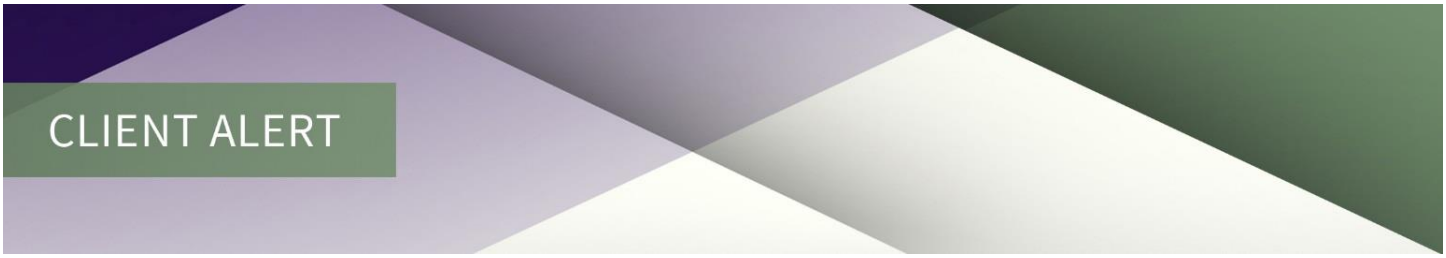

Convergence of Antitrust and Privacy: Bedoya's Confirmation to FTC Moves the Process Forward

September 7, 2022

AUTHORS

Daniel K. Alvarez | Michelle Clark | Laura E. Jehl | William H. Rooney
Amelia Putnam

The Federal Trade Commission ("FTC") under Chair Lina Khan has taken a number of steps that signal significant changes to the way the agency approaches data privacy and data protection regulation. These activities have ramped up since the confirmation earlier this summer of Commissioner Alvaro Bedoya, who provides the critical "third" Democratic vote on the FTC that solidifies Chair Khan's majority and allows her to move forward with her agenda on privacy and other consumer protection issues. The FTC's adoption of an Advance Notice of Proposed Rulemaking on "harmful commercial surveillance" and "lax data security" practices, which we discuss here[1] is the latest and most significant step on this front so far.

Longer term, however, the partnership between the FTC's two newest members — Khan, an antitrust expert, and Bedoya, a privacy expert — suggests the possibility of a convergence of traditional privacy and antitrust concepts as a way to address the issues on the FTC's agenda, one that is already well underway in other jurisdictions, particularly in the European Union. This convergence may come sooner than expected — the Advance Notice specifically references the role of privacy and data protection regulation in promoting competition.

[1] *Federal Privacy Rules on the Horizon? FTC Begins Rulemaking on Commercial Surveillance and Data Security Practices*, WILLKIE FARR & GALLAGHER LLP (Aug. 15, 2022), here.

The FTC's Tools to Regulate Privacy and Antitrust

The FTC's structure reflects its traditional bifurcation of antitrust and competition on the one hand, and consumer protection and privacy on the other. Today, the majority of FTC staff are divided between two bureaus: the Competition Bureau and the Consumer Protection Bureau.[2] The Competition Bureau exercises the FTC's authority with respect to antitrust and competition laws. The Consumer Protection Bureau focuses on consumer protection and any laws that the FTC is charged with enforcing in that space, including with respect to privacy and data protection.

Recently, the FTC was given the opportunity to evaluate how its antitrust authority can be used to regulate privacy issues. Accountable Tech, an organization focused on advocating for regulations protecting personal data collection by social media companies, petitioned the FTC to ban what the petition refers to as "surveillance advertising" as an unfair method of competition.[3] Using traditional antitrust concepts and language, the petition argues that there is a symbiotic relationship between the collection of large amounts of personal information and anticompetitive behavior by firms that amass those troves of data; large companies have increased their personal data collection and have used "exclusive dealing" to create competitive barriers for other social media companies to access such personal data and increase their market share.[4] Accountable Tech describes "exclusive dealing" as the exclusion by dominant companies of competitors from access to personal data by "flatly deny[ing] rivals access to the essential chokepoints they control."[5]

The FTC sought public comments on the petition and, on August 11, 2022, issued an Advance Notice of Proposed Rulemaking Regarding Commercial Surveillance and Data Security ("Advance Notice").[6] In Footnote 47 of the Advance Notice, the FTC mentions Accountable Tech's petition and seeks public comment "on the ways in which existing and emergent commercial surveillance practices harm competition and on any new trade regulation rules that would address such practices."[7] While the FTC's Advance Notice addresses the regulation of commercial surveillance using consumer protection concepts, the FTC has also signaled that it is considering how its antitrust and consumer protection authorities may overlap to regulate privacy and data security.

---

2 *Bureaus & Offices*, FEDERAL TRADE COMMISSION, here (last accessed Sept. 2, 2022).

3 *Re: Petition for Rulemaking to Prohibit Surveillance Advertising*, ACCOUNTABLE TECH (Sep. 28, 2021), here.

4 *Id.* at 19–57.

5 *Id.* at 51.

6 *Trade Regulation Rule on Commercial Surveillance and Data Security*, 16 C.F.R. 464, FTC (Aug. 11, 2022), here. For more information about this Advance Notice, please see here.

7 Advance Notice, at 10.

The Convergence of Privacy and Antitrust Concerns in Europe

The wall between antitrust and privacy concerns has been eroding for several years. For example, in 2019, Alden Abbott, at the time the FTC's General Counsel, argued that the possession and use of "big data" can be a barrier to competition that chills innovation.[8] Abbott explained that some companies can exclude other companies from using personal data to leverage their own monopolistic position in digital markets, thereby harming both consumers and competition.[9] This line of argument appears to have found a receptive audience in Chair Khan.

In Europe, competition law focuses on illegal agreements and abuses of dominance. The categories of abuse of dominance have expanded significantly in recent years to deal with issues arising in digital markets. In relation to data protection, the General Data Protection Regulation (the "GDPR") came into force across Europe in 2018 and is considered a far-reaching and ambitious privacy regulation.

Europe has sought to complement competition law and the GDPR with further regulations aimed at addressing both competition and privacy issues specific to digital markets and Big Tech. For example, the European Commission has proposed a Digital Markets Act ("DMA"), which is scheduled to come into force across Europe (save for the UK given Brexit) in October of this year. The DMA applies to large online platforms that meet particularly high turnover and user-number thresholds, which are referred to as "gatekeepers." We expect that all of the world's largest platforms will be designated as gatekeepers.[10]

The DMA prohibits gatekeeper platforms from engaging in a number of "unfair practices," including self-preferencing and using nonpublic data generated by businesses when using the gatekeeper's platform.[11] The DMA also prohibits activities that are more characteristic of traditional privacy regulation, such as prohibiting gatekeepers from tracking end users

---

8 Alden Abbott, *Big Data and Competition Policy: A US FTC Perspective*, here (last accessed Sept. 2, 2022).

9 *Id.* Interestingly, some parties have used privacy and security concerns as an argument *against* certain antitrust activities. For example, as Congress has increased its antitrust legislative efforts targeting Big Tech companies, cybersecurity and privacy concerns are often cited by opponents of these bills who argue that the legislation hinders companies' ability to protect privacy and cybersecurity for their customers. *See, e.g.*, Emily Birnbaum, *Revised Tech Antitrust Bill Attempts to Address Privacy, Cybersecurity Concerns*, POLITICO (May 26, 2022). Despite pushback from Big Tech companies, there is still reason to believe that Congress may enact antitrust legislation that would also have important privacy implications. *See* Lauren Feiner, *Lawmakers Are Racing to Pass Tech Antitrust Reforms Before Midterms*, CNBC (June 6, 2022), here.. For example, the American Innovation and Choice Online Act, which is primarily an antitrust bill, prohibits large online platforms from "materially restrict[ing] or imped[ing] a business user from accessing data generated on the covered platform by the activities of the business user . . . by establishing contractual or technical restrictions that prevent the portability by the business user to other systems or applications of the data of the business user." *See* Victoria Hudgins, *Big Tech Antitrust Bill Could Create Data Sharing Requirements*, GLOBAL DATA REVIEW (Aug. 16, 2022), here.

10 *The Digital Markets Act: Ensuring Fair and Open Digital Markets*, EUROPEAN COMMISSION, here (last accessed Sept. 2, 2022).

11 *Id.*

outside of the platform in order to collect personal data for targeted advertising purposes without the end user's consent (i.e., "off-platform" collection of data).[12] The DMA also regulates user consent, and requires mechanisms to be put in place to ensure that users must be able to refuse consent to their personal data being used, and that such refusal should be made as easy as granting consent, and, in cases where consent is refused, requests cannot be repeated for one year.

The DMA thus represents a new level of convergence of European competition and privacy law and may serve as an example for U.S. regulators.

The Implications of the FTC's Privacy and Antitrust Agendas

The convergence of antitrust and privacy issues may presage two possible regulatory developments — the use of antitrust concepts to improve privacy outcomes, and using access to data to improve antitrust outcomes, with implications for privacy. As to the former, the FTC may treat business activities that result in a seller's amassing, or encourage a seller to amass, troves of data about individuals as anticompetitive or otherwise unfair methods of competition. Such an FTC initiative could have significant implications for companies' incentives to collect that data in the first instance (for example, as with the "adtech" business model).

Additionally, the FTC may assert that greater user access to data — and greater user control over their own data — can facilitate better competitive outcomes. That view, for example, is one of the primary justifications for the data portability requirements in laws like the GDPR. Consumer rights, including data portability, "could theoretically reduce the switching costs consumers face, for example if they must reproduce all of the information and content inputted into a digital content platform whenever they switch providers."[13] Greater user access to, and control over, personal data has also been proposed by some parties as one potential remedy in response to allegations of anticompetitive conduct by larger Internet platforms.[14] Of course, these solutions have significant privacy implications because they often result in data multiplication, not data replacement.

---

12 *Id.*

13 *Data Portability, Interoperability and Competition*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, here (last accessed Sept. 2, 2022).

14 *See, e.g.*, *A New Competition Framework for the Digital Economy*, GERMAN FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND ENERGY, COMMISSION "COMPETITION LAW 4.0," here (last accessed Sept. 2, 2022) ("The Commission's 'Competition Law 4.0' takes the view that the strengthening of consumer autonomy can be an important instrument to facilitate access to consumer data and to avoid the emergence of competition problems. The easier it is for consumers to transfer their data from one provider to another or to grant new providers access to data, the easier it will be for rival companies to attack data-based market power. For this reason, it is proposed that the existing right to data portability in data protection legislation be tightened for dominant platforms."); Bennett Cyphers and Cory Doctorow, *Privacy Without Monopoly: Data Protection and Interoperability*, ELECTRONIC FRONTIER FRONT (Feb. 12, 2021), here ("Data portability gives users the right to access and transfer their data from the companies that hold it. Back-end interoperability would require very large companies—those that dominate a particular market segment—to

Conclusion

The FTC has demonstrated interest in regulating privacy and data security, and Commissioner Bedoya will likely be the leading voice at the FTC on those issues. Now that Chair Khan has a clear majority to push forward with her agenda (a majority that will be further solidified by the expected departure of Republican Commissioner Noah Phillips this fall), the FTC will likely attempt to use its antitrust authority to more aggressively regulate privacy issues.

Such an initiative is likely to be supported by Commissioner Bedoya, particularly because he has deep experience in privacy and surveillance issues.[15] Combined with Chair Khan's expertise in antitrust law,[16] the FTC has the tools to regulate privacy issues in novel ways. Companies, particularly those involved in digital markets or advertising, should be alert to additional rulemaking and enforcement activities involving privacy and antitrust law, which would almost certainly significantly affect competition in many tech markets.

maintain interfaces that allow their users to interact fluidly with users on other services. . . . Making it easier for new entrants to create privacy-preserving alternatives will pressure incumbents to do better, and allow users to migrate away when they don't."); Mark Zuckerberg, *Four Ideas to Regulate the Internet*, FACEBOOK NEWSROOM (Mar. 30, 2019), here ("Finally, regulation should guarantee the principle of data portability. If you share data with one service, you should be able to move it to another. This gives people choice and enables developers to innovate and compete.").

15 *Georgetown Law Center on Privacy & Technology*, here (last accessed Sept. 2, 2022).

16 Prior to joining the FTC, then-Professor Khan published a law review article discussing the ways in which Big Tech companies have used their monopoly power and data collection practices in harmful, codependent ways. *Sources of Tech Platform Power*, 2 GEORGETOWN LAW & TECHNOLOGY REVIEW 325 (2018). For example, she explained that certain platforms "engage in information exploitation against the businesses that use their services to reach markets." *Id.* at 329. To address this issue, she called for regulations similar to the GDPR because such regulations limit the amount and types of personal data that companies may collect and could serve to hinder "platforms from using information collected on their platforms to advantage distinct lines of business." *Id.* at 333.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Michelle Clark
+44 203 580 4737
mcclark@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

William H. Rooney
212 728 8259
wrooney@willkie.com

Amelia Putnam
202 303 1089
aputnam@willkie.com