Comments for the Record

Commercial Surveillance ANPRM

JEFFREY WESTLING, JOSHUA LEVINE | OCTOBER 26, 2022

I. Introduction & Summary

The Federal Trade Commission (FTC) has a long and important history protecting consumers from unfair and deceptive acts or practices. As a part of this mission, the FTC rightly targets abusive practices from firms regarding the collection and use of user information and data, primarily through consent decrees and ad hoc enforcement actions.[1] As Congress contemplates the development of a national privacy framework, the Commission stands ready to act as the cop on the beat to protect consumers.[2]

This Advanced Notice of Proposed Rulemaking[3] departs from the Commission's previous actions to protect consumer privacy. Rather than relying on its traditional enforcement tools, the agency instead seeks to establish ex ante rules prohibiting specific conduct such as using data to target advertising to consumers or requiring that firms establish safeguards to protect data controlled by the firm.[4]

Congress imposed significant restrictions on the use of rulemaking authority to develop rules and regulations regarding the specific types of conduct that could constitute unfair or deceptive acts or practices.[5] As Congress has made clear, FTC may only pass rules addressing practices that are likely to cause substantial injury to consumers and not outweighed by benefits to consumers or to competition.[6] Further, even if a practice could constitute a violation of Section 5, the Commission may only use rulemaking after considering alternative methods for achieving such objectives.[7]

If the Commission attempts to create a broad privacy regime using Section 18 authority, the regulations would likely run afoul of the act and be struck down by the courts. Many of the harms associated with privacy violations don't meet the statutory definitions, and evidence from other privacy regimes across the globe highlight the significant consumer benefits that may be lost.[8] Further, current ex post enforcement provides significant protection for consumers, stopping many of the most harmful practices companies have engaged in and dissuading firms from pushing the bounds of the law too far.[9] If Congress wanted the FTC to develop a complete privacy regime, it could do so. But absent that clear authority from Congress, a blanket privacy regime would likely run afoul of the major questions doctrine.[10]

If, however, the Commission seeks to impose some narrowly tailored regulations regarding a few specific unfair or deceptive acts or practices, it may be able to do so. But again, the agency will need to show that the practices in question cause significant consumer harms not outweighed by the benefits.[11] Many of the issues identified by the Commission provide significant benefits to consumers, and these benefits cannot be dismissed lightly.

As the Commission continues to work through this process, it should carefully balance the alleged harms with the proven benefits to consumers and competition. While the Commission should protect consumer privacy, overbroad and expansive rules could do more harm than good. If the United States needs more ex ante prohibition, Congress should pass a national privacy framework that retains the FTC's role as the cop on the beat to protect consumers.

II. The Commission Does Not Have the Authority to Issue Broad-Sweeping Privacy Regulations on the Entire Economy

At the outset, the Commission must contend with the difficult task of showing it has the authority to issue privacy rules under Section 18 of the FTC Act.[12] While Congress did grant the agency the authority to pass rules regarding unfair and deceptive acts or practices, the more broadly the Commission interprets this grant of authority, the more likely it will be to run into legal challenges.

Primarily, the FTC will need to show that the practices defined unlawful by rule are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[13] Further, Section 18 makes clear that the FTC should consider alternatives to rulemakings in preventing these practices.[14] Finally, even if the FTC can successfully show that a rule prohibiting a particular practice fits these requirements, recent guidance from the Supreme Court casts some doubts on the FTC's authority to pass wide-sweeping privacy regulations without direct authority from Congress.

A. Many of the privacy concerns outlined in the ANPRM are not likely to cause substantial injury to consumers.

The ANPRM primarily focuses on the collection and use of user data, and while there could certainly be some harms associated with specific practices, the majority of harms related to user data stem from lax data security. For example, the ANPRM highlights the myriad ways a firm can collect user data and use it in ways that consumers may not expect or agree to. While these practices could lead to some consumer harm, the use of data for personalized ads or the lack of control of the data by the user doesn't in isolation create the substantial injury to consumers that the FTC normally seeks to target. Instead, as the Commission acknowledges in the overview section of the ANPRM, the potential substantial risks occur primarily due to "lax security practices" and risks of cyberattack by hackers, data thieves, and other bad actors.[15]

While the Commission raises concerns about the asymmetry of data and the large quantity of data collected, the collection of data itself doesn't give rise to the substantial harms that the FTC Act outlines. If Congress wants to limit the collection and use of data, it can and will do so. The Commission, however, is bound by the statute and therefore should use this proceeding to primarily focus on data security rather than a broader inquiry about the collection and use of data that will not likely cause substantial risk to consumers.

Even then, the Commission will need to show that specific data security practices will likely lead to significant harms to consumers. As the International Center for Law and Economics highlights, the FTC's enforcement actions regarding data security often lack the economic analysis that would show harms to consumers.[16] For example, in giving employees administrative control over Twitter systems, the FTC alleged that Twitter increased the risk of a serious breach without any examination of that increased risk.[17] In a complaint involving a firm that didn't inspect outgoing transmissions for unauthorized disclosure of personal information, the FTC concluded that monitoring these transmissions could have reduced the risk of data compromise or the breadth thereof.[18] The vague and arbitrary view of the requirement that a practice is likely to cause substantial injury can lead to inconsistent and unclear standards for companies to adhere to. The ANPRM presents a good opportunity to collect data on these potential harms so that the Commission can undergo a rigorous analysis before issuing specific regulations.

Proving substantial harms will undoubtedly be a difficult task for the Commission as it works through the

rulemaking process.[19] As a result, the Commission should focus its efforts on considering and analyzing data security practices rather than specific collection or use practices that almost certainly won't lead to provable consumer harms absent a data breach or some other cybersecurity incident. If the Commission attempts to use this process to develop a broad, wide-sweeping privacy regime that covers the collection and use of user data, it could forgo meaningful improvements on cybersecurity standards and practices within the industry.

B. Existing comprehensive privacy regulations in other countries have eliminated significant consumer benefits that may outweigh any harms derived from the collection and use of data.

Even if the Commission can show significant harm to consumers, the statute requires the Commission to consider the potential benefits that regulation could eliminate. Indications from privacy regimes across the globe highlight the significant benefits consumers and businesses could lose with overly broad requirements.

In the ANPRM, the Commission illustrates how countries around the world have enacted laws and regulations that impose restrictions on companies' collection, processing, retention, transfer, sharing, and sale or other monetization of data.[20] The European Union's General Data Protection Regulation (GDPR), for example, limits the lengths firms can go to collect personal data and gives consumers substantial rights to restrict the collection, use, and processing of their data online.[21] While these restrictions may limit some potential harms, they actively curtail the benefits of data collection and use.

For firms operating in the digital economy, data collection, processing, and analysis help them improve their products to better serve consumers.[22] Restricting data collection, processing, and sharing prevents firms from enjoying the positive synergies created by data collection, such as providing users with new and curated services allowing firms to further monetize and tailor their content.[23] This new reality could have negative effects on the formation of businesses and innovations that rely on large data sets, such as Artificial Intelligence (AI), further depriving consumers of valuable services they might wish to use.[24]

Broad privacy regulation could also stifle the development of new and competitive services to challenge currently dominant firms in the technology sector. For example, research shows that since the incorporation of the GDPR in Europe, there has been an increase in market concentration in web technology services, with Google gaining more than four times the market share of the next closest company, Facebook.[25] In fact, following the introduction of the GDPR, the number of new apps and technology firms fell by 47.2 percent, creating a "lost generation" of available apps.[26] This decline can be traced directly to the GDPR: Europe has seen a decrease in the use of third-party domain services that help track and collect data on users,[27] and instead, firms have kept data remains siloed in one organization. This puts new entrants and smaller firms at a potential disadvantage due to their lack of access to user data.[28] As a result, European consumers, and indeed consumers across the globe, lose out on the benefits that can come with disruptive innovation in the technology sector.

If the Commission were to adopt rules that take guidance from the framework of the GDPR, it may reduce competition, harm new entrants and innovation, and limit the consumer benefits technology services provide. The statute clearly requires that the Commission balance the potential harms to consumers against the benefits of these practices, and broad privacy regulations modeled after regimes like the GDPR would curtail many of the benefits outlined above.

C. The Commission has alternative tools for enforcement that adequately protect consumers from unfair or deceptive practices regarding the collection and use of user data.

As required by law, the FTC must seek feedback and consider alternative methods for achieving the objectives laid out in the ANPRM. According to the Commission, case-by-case enforcement of unfair and deceptive acts or practices falls short for four reasons: 1.) a lack of civil penalty authority for initial violations; 2.) injunctive relief may be inadequate in the context of privacy; 3.) difficulty in applying monetary damages to privacy harms; and 4.) the Commission's lack of resources necessary to adequately protect consumers.[29] None of these reasons adequately justifies broad privacy rules.

First, while the FTC lacks civil penalty authority for first-time violations, it can still use injunctive relief through case-by-case adjudication to highlight the types of conduct that could lead to FTC enforcement.[30] Firms do not want to come under investigation by the FTC, as an investigation (especially one where guilt is found) can produce reputational harms for the firm. As the FTC, through case-by-case adjudication, lays out clear practices that violate Section 5, firms are less likely to engage in those practices, ultimately limiting the risk of significant harm to consumers.[31]

Second, the Commission is right that injunctive relief doesn't provide remediation for consumers harmed by lax data security practices, but such relief does, to some degree, prevent potential future harms by laying out the specific practices that violate the act. The purpose of Section 5 is to protect consumers from unfair or deceptive acts or practices, and the robust record of FTC privacy enforcement suggests that consumers are being protected from significant injury.[32]

Third, the Commission is right that it can be difficult to quantify privacy harms, but that further indicates the need for Congress to establish a national privacy framework. Congress clearly expressed skepticism about FTC rulemaking, and the agency doesn't have carte blanche to issue rules untethered from an analysis of the actual harm to consumers.[33] While quantifying harm can be difficult, it is not impossible, and when a firm violates a consent decree, the Commission can seek monetary damages to punish the bad actor. If the Commission needs additional authority, Congress should give clear guidance on how the FTC should see monetary damages for specific conduct.

Finally, many have called for additional resources for the agency to better protect consumer privacy. If the Commission needs additional resources to investigate practices and bring claims, Congress should grant the agency those resources. In fact, there has been discussion in Congress about increasing FTC resources through updates to the merger filing fees.[34] Yet a lack of resources doesn't give the agency authority to substantively change the legal standards for Section 5 violations.

D. The major questions doctrine puts the onus on Congress to develop a comprehensive privacy regulation.

Finally, even assuming the Commission can satisfy the requirements of its rulemaking authority, recent jurisprudence on the major questions doctrine highlights a growing skepticism of agency overreach. In *West Virginia v. EPA*, the Supreme Court explained that the agencies cannot make rules with major economic or political significance without clear authority from Congress.[35] In the decision, the Court relied on the idea that the FTC discovered broad regulatory power in a largely unused statute.[36] Here, Congress clearly granted the FTC authority to issue rules defining unfair or deceptive acts or practices. If the Commission attempts to create a broad regulatory regime governing the collection and use of consumer data, however, the entire regime could be struck down on major questions grounds.

Instead, as detailed above, the Commission should focus on specific cases where data security standards or rules against specific collection and use of data may prevent practices that lead to significant harms to consumers that they cannot reasonably avoid. To put it more bluntly, the Commission should be very careful not to use its rulemaking authority too broadly, as the statute itself was designed to curtail agency authority, not expand it.

III. Even Narrowly Tailored, Rules Prohibiting Specific Conduct Outlined in the ANPRM Could Fail to Meet the Statutorily Required Standard of Proof Due to Limited Harms and Significant Consumer Benefits

As the Commission evaluates targeted rules, a few questions deserve further attention. While the Commission shouldn't use the rulemaking process to develop a comprehensive privacy regime, it may be able to use this opportunity to develop narrow regulations targeting specific practices that give rise to significant consumer harms. Many of the practices outlined in the ANPRM provide significant benefits, however, and the Commission should carefully weigh these potential benefits against the threats of harm, as required by the statute, before issuing any ex-ante rules.

A. Targeted Ads

The Commission asks a multitude of questions related to targeted advertising and whether alternative advertising models compare to targeted ads.[37] Targeted advertising creates a mutually beneficial exchange of information by targeting consumers who may be interested in a company's products based on previous activity and providing a more personalized online experience for users. Companies utilizing online ads rely on "online behavioral advertising" a practice which allows firms to personalize and target advertisements. The ability for sites to collect, share, and process data allows this ecosystem to flourish by leveraging ad data to further personalize content, and websites rely on ad revenue rather than fees from consumers to function.[38] Preventing the continued development and evolution of targeted online advertising would disrupt the current online experience and prevent the mutually beneficial exchange of information.

Conversely, rules that prevent the use of online consumer data to target and craft advertisements will drive inefficiencies in the ad space, could subject consumers to more ads, and potentially lead to fewer free online services or perks that drive current internet use. After the introduction of the GDPR's rules around data collection, sharing, intermediary liability, and consent requirements, websites reduced their connections to web technology providers, with a particular focus on personal data.[39] Research predating the GDPR has shown that increased privacy restrictions in Europe coincided with a 65% reduction in effectiveness for banner ads, a common and basic ad type, especially when used on general websites, like news sites.[40] Following the introduction of the GDPR, firms abandoned products in lieu of adopting onerous compliance measures, small- and medium-sized firms have seen costs rise and revenues fall while large firms such as Google have increased their market share, and the absence of ad revenue could lead to more services moving to a subscription or paid model to make up for lost revenues.[41]

B. Algorithmic Decision Making

The Commission's questions on algorithmic decision-making are broad and touch on several areas where algorithms are employed to increase efficiency and improve the user experience online. Algorithms are employed by search engines, social media platforms, and other technology service providers to help with indexing content, content moderation, data analysis, and other tasks. Recently, there have been pushes to restrict the development and use of algorithms due to concerns over transparency, fairness, equity, and accountability.[42]

These are worthy concerns, but the Commission should not translate these concerns into restrictive regulations. Courts have ruled that algorithms are protected speech,[43] and Section 230 of the Communications Decency Act protects the use of algorithms to help moderate and index content.[44] Industry, academia, and civil society are developing soft law approaches to ensure researchers and firms balance the potential risks posed by these technologies while not restricting innovation.[45]

C. Biometric Information

The Commission asks whether it should "consider limiting commercial surveillance practices that use or facilitate the use of facial recognition, fingerprinting, or other biometric technologies."[46] If biometric data fall into the wrong hands, consumers could face real risks. Consumers cannot change their biometric information, and therefore malicious use of this information could lead to increased risk of identity theft or other types of harm.[47] When contemplating whether a regulation is needed to prevent harms to consumers, the limited remediation options after a breach could justify ex ante rules.

At the same time, there are many benefits to using biometric data. Biometric identification and authentication generally provide more security for the user because forging that information is much more difficult.[48] Tokens can be duplicated or passwords can be weak, but biometric features are unique and difficult to replicate. The efficiency of biometrics makes it easier for consumers to be more secure with their information. While the risks of a breach involving biometric information could be significant, the benefits of the collection and use of biometric information may be even greater. The Commission should carefully consider these relative costs and balances.

D. Integration of Services

The Commission further asks if it should "limit companies that provide any specifically enumerated services

from owning or operating a business that engages in specified commercial surveillance practices like personalized or targeted advertising."[49] The Commission should not impose any such rule, as significant consumer benefits can come with integration, and instead the Commission should rely on case-by-case adjudication for any potential violation of section 5.

Integration allows firms to generate efficiencies that are then passed on to consumers.[50] If a firm provides a search engine and engages in targeted advertising based on those search results, the firm can invest more resources into improving its engine while also delivering ads to consumers that will provide value to consumers. Likewise, a social media company can deliver advertisements to users based on the needs and characteristics of that user, all while providing a valuable platform for dialogue at no cost to consumers. If the Commission places large barriers on these firms, the quality of their product would likely decline as the firm has less resources to invest in research, development, and overall improvements to their services. In the end, consumers lose out.

Further, such a rule would essentially be an antitrust rule masquerading as a privacy rule. The consumer welfare standard requires a careful examination of the relative costs and benefits to consumers when evaluating whether a practice or acquisition is anticompetitive.[51] The Commission shouldn't seek to circumvent the consumer welfare standard in favor of a "big is bad" approach to competition policy, but even if it does, it shouldn't do so in a privacy rulemaking proceeding.

E. Data Minimization

The Commission asks whether rules related to data minimization would "protect consumer data security," "unduly hamper algorithmic decision-making or other algorithmic learning-based processes or techniques," whether such rules would be administrable, and potential impacts on consumers access to free or reduced-cost services if data minimization rules went into effect.[52] Data minimization restricts firms from collecting user data unless it is necessary to meet specific business needs, which would likely increase consumer data security at the expense of new products, companies, and innovations. The GDPR includes provisions that require data minimization practices as well as consent from users for any use of collected data. Following the GDPR's introduction, researchers found a 12.5 percent reduction in total cookies, a clear decrease in trackable and monetizable data for firms.[53] This decrease has coincided with a marked decline in new firms and products, increased compliance costs for existing firms, fewer investments in new technology startups in Europe, and concerns that data minimization will effectively eliminate Europe's ability to produce innovation in AI.[54]

Data minimization rules could pigeon-hole firms into specific practices and restrict their ability to adapt to new market environments and pursue innovation. Innovation and growth require the ability to experiment and fail, and data minimization rules make experimentation and failure incredibly costly endeavors. The Commission should carefully consider these tradeoffs when exploring data minimization requirements.

F. Consent

The Commission asks several questions about the administrability, importance, and breadth of consumer consent for data collection and "commercial surveillance." The Commission also asks if consumer consent is "an effective way of evaluating whether a practice is unfair or deceptive."[55] Consumer consent to data collection and tracking is often the default in the United States, and consumers can opt-out of certain cookies and data tracking practices, whereas in Europe the GDPR requires consumers to opt-in to tracking by any website they visit and provide additional consent for every use of data outside the initial consent. The Commission should not adopt rules that shift the status quo from opt-out to opt-in in the United States and

should focus on specific instances where companies fail to secure user data appropriately or misuse the data to tangibly harm consumers.

By relying on an opt-out rather than an opt-in regime, technology service providers offer an avenue for data-privacy concerned users to protect their data, but still allow robust data collection to drive innovation and consumer benefits. Estimates of the cost of reducing access to data with opt-in consent requirements rather than opt-out would cost the United States economy $71 billion annually.[56] By switching to an opt-in requirement, regulators increase compliance costs in the form of additional staff and processes to handle user data, as well as hidden costs, exemplified in lost opportunities for data to drive innovation and consumer benefits.[57]

There is little evidence that switching to an opt-in consent requirement significantly benefits consumers, but there is evidence it imposes greater costs on them by having to opt-in or out every time they use an online service and is shown to discourage sharing data with new entrants.[58] The Commission should be more specific about what types of collection and types of data it wants to protect and understand that efforts to require greater consent and scrutiny come with substantial costs in the short and long-term.

Conclusion

Protecting consumers from unfair or deceptive acts and practices regarding the collection, use, and management of data should remain a key priority for the Commission. A rulemaking, however, must be narrowly tailored to address significant harms to consumers without eliminating countervailing benefits. As the Commission continues to build a record in this proceeding, we urge the agency to carefully consider the benefits of any practices it wishes to prohibit, and refrain from developing a comprehensive privacy regime through rulemaking, as this should instead be accomplished through congressional legislation.

***

Respectfully submitted,

/s/

Jeffrey Westling

Director, Technology & Innovation Policy

The American Action Forum

1747 Pennsylvania Avenue, N.W.

Washington, D.C. 20006

Joshua Levine

Analyst, Technology & Innovation Policy

The American Action Forum

1747 Pennsylvania Avenue, N.W.

Washington, D.C. 20006

Oct. 26, 2022

[1] Report to Congress, *FTC Report to Congress on Privacy and Security*, Federal Trade Commission (Sept. 13, 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

[2] Jeffrey Westling, *Could Congress Finally Move on Privacy?*, American Action Forum (June 15, 2022), https://www.americanactionforum.org/insight/could-congress-finally-move-on-privacy/.

[3] Advanced Notice of Proposed Rulemaking, *Trade Regulation Rule on Commercial Surveillance and Data Security*, Federal Trade Commission (Aug. 11, 2022) ("ANPRM"), https://www.ftc.gov/system/files/ftc_gov/pdf/commercial_surveillance_and_data_security_anpr.pdf.

[4] *Id*. at p. 22.

[5] Dan Bosch, *Primer: The FTC and Magnuson-Moss Rulemaking*, American Action Forum (Sept. 21, 2022), https://www.americanactionforum.org/insight/primer-the-ftc-and-magnuson-moss-rulemaking/.

[6] 15 U.S.C. § 45(n).

[7] 15 U.S.C. § 57a(b)(2).

[8] Rebecca Janßen et al., *GDPR and The Lost Generation of Innovative Apps*, NBER Working Paper Series (May 2022), https://www.nber.org/system/files/working_papers/w30028/w30028.pdf.

[9] "Congress has given the Commission the enforcement and policy tools to provide a strong framework with

which we can protect American Consumers." Statement of Maureen K. Olhausen, Commissioner, Federal Trade Commission Before the Senate Committee on Commerce, Science and Transportation, *Hearing on "The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission"* p. 3 (May 9, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120509privacytestimony.pdf.

[10] Jeffrey Westling, *Major Questions Doctrine and the Impact on Biden's Technology Priorities*, American Action Forum (July 14, 2022), https://www.americanactionforum.org/insight/major-questions-doctrine-and-the-impact-on-bidens-technology-priorities/#:~:text=In%20West%20Virginia%2C%20one%20key,clear%20statutory%20authorization%20from%20Cong
.

[11] 15 U.S.C. § 45(n).

[12] 15 U.S.C. § 57a.

[13] 15 U.S.C. § 45(n)

[14] 15 U.S.C. § 57a(b)(2).

[15] ANPRM at p. 7.

[16] Geoffrey A. Manne and Kristian Stout, *When "Reasonable Isn't: The FTC's Standardless Data Security Standard*, 15 Journal of Law Economics & Policy p. 67 (2018), https://static1.squarespace.com/static/6233d0b9d24b954d519e5d62/t/626b520965046b4f5e79a8f3/1651200529209/V.15
.

[17] *Id*. at p. 68.

[18] *Id*.

[19] Cobun Keegan & Calli Schroeder, *The FTC's Evolving Measures of Privacy Harms*, 15 Journal of Law, Economics & Policy p. 19 (2018), https://static1.squarespace.com/static/6233d0b9d24b954d519e5d62/t/626b520965046b4f5e79a8f3/1651200529209/V.15
.

[20] ANPRM at pp. 10-12.

[21]*Id* at p. 21.

[22] Andres V. Lerner, *The Economics of Network Effects and User Data in the Provision of Search, Search Advertising, and Display Ad Intermediation*, Australian Competition and Consumer Commission p.21 (May 15, 2019), https://www.accc.gov.au/system/files/Google%20Submission%203%20%28May%202019%29.pdf.

[23] *Id* at pp. 20-21; Oshrit Aviv and Michal S. Gal, *The Competitive Effects of the GDPR*, 16 Journal of Competition Law and Economics p.28 (Mar. 4, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548444.

[24] Knut Blind et al., *How Data Protection Regulation Affects Startup Innovation*, 21 Information Systems Frontiers pp.1318-19 (2019), https://link.springer.com/article/10.1007/s10796-019-09974-2.

[25] Michail Batikas et al., *European Privacy Law and Global Markets for Data*, CEPR Discussion Paper No. DP14475 p.26 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3560282.

[26] Rebecca Janßen et al., *supra* n. 9, at pp.3-4.

[27] Batikas et al., *supra* n. 26 at pp. 24-25.

[28] *Id* at pp.23-26.

[29] ANPRM at pp. 22-23.

[30] 15 U.S.C. § 45.

[31] 15 U.S.C. § 45(l).

[32] *FTC Report to Congress on Privacy and Security*, Federal Trade Commission (Sept. 13, 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

[33] Dan Bosch, *Primer: The FTC and Magnuson-Moss Rulemaking*, American Action Forum (Sept. 21, 2022), https://www.americanactionforum.org/insight/primer-the-ftc-and-magnuson-moss-rulemaking/.

[34] Ashley Gold, *House passes bill to raise DOJ, FTC merger fees*, Axios (Sept. 29, 2022), https://www.axios.com/2022/09/29/house-bill-raise-merger-fees-doj-ftc.

[35] West Virginia v. Environmental Protection Agency, 20-1530 (slip opinion) (2022), https://www.supremecourt.gov/opinions/21pdf/20-1530_n758.pdf.

[36] *Id*. at p. 20.

[37] ANPRM at pp. 39 – 43.

[38] Simone Aiolfi, Silvia Bellini, Davide Pellegrini, *Data-Driven Digital Advertising: Benefits and Risks of Online Behavioral Advertising*, International Journal of Retail & Distribution Management p.1091 (2021), https://www.emerald.com/insight/content/doi/10.1108/IJRDM-10-2020-0410/full/html; Michael Wedel and P.K. Kannan, *Marketing Analytics for Data Rich Environments*, Journal of Marketing pp. 97-121 (2016), https://journals.sagepub.com/doi/10.1509/jm.15.0413; P.K. Kannan and Hongshuang (Alice) Li, *Digital Marketing: A Framework, Review and Research Agenda*, 34 International Journal of Research in Marketing p.25 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000712; Alan McQuinn, *The Detractors are Wrong, Online Ads Add Value*, Information Technology and Innovation Foundation (2016), https://itif.org/publications/2016/12/08/detractors-are-wrong-online-ads-add-value/

.

[39]Michail Batikas et al., *supra* n. 26, at pp.13-16.

[40] Avi Goldfarb and Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 Management Science p.3 (2010), https://pubsonline.informs.org/doi/abs/10.1287/mnsc.1100.1246.

[41] Canadian Marketing Association, *Privacy Law Pitfalls: Lessons Learned from the European Union* (2022), https://thecma.ca/docs/default-source/default-document-library/cma-2022-report-privacy-legislation-pitfalls.pdf?sfvrsn=ed54bdf4_6.

[42] Martin Austermuhle *D.C. Attorney General Introduces Bill to Ban 'Algorithmic Discrimination*, NPR (Dec. 10, 2021), https://www.npr.org/local/305/2021/12/10/1062991462/d-c-attorney-general-introduces-bill-to-ban-algorithmic-discrimination.

[43] Alison Dame-Boyle, *EFF at 25: Remembering the Case that Established Code as Speech*, Electric Frontier Foundation (Apr. 16, 2015), https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech.

[44] Daniel Castro and Alan McQuinn, *A Grand Bargain on Data Privacy Legislation for America*, Information Technology and Innovation Foundation p.22-23 (Jan. 2019), https://www2.itif.org/2019-grand-bargain-privacy.pdf.

[45] Carlos Ignacio Gutierrrez & Gary Marchant, *A Global Perspective of Soft Law Programs for the Governance of Artificial Intelligence,* Arizona State University (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855171.

[46] ANPRM at p.31.

[47] Alan S. Wernick, *Biometric Information – Permanent Personally Identifiable Information Risk*, American Bar Association (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/

[48] Sterling Miller, *The basics, usage and privacy concerns of biometric data*, Thomas Reuters (July 20, 2022), https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data.

[49] ANPRM at p. 31.

[50] Jeffrey Westling & Juan Londoño, *The Effect of Congressional Antitrust Legislation on Consumers*, American Action Forum (Jan. 18, 2022), https://www.americanactionforum.org/insight/the-effect-of-congressional-antitrust-legislation-on-consumers/.

[51] Fred Ashton, *Why the Consumer Welfare Standard Is the Backbone of Antitrust Policy*, American Action Forum (Oct. 26, 2022), https://www.americanactionforum.org/insight/why-the-consumer-welfare-standard-is-the-backbone-of-antitrust-policy/.

[52] ANPRM at 45 – 51

[53] Guy Aridor, Yeon-Koo Che & Tobias Salz, *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR*, NBER Working Paper No. 26900 p.3 (Mar. 2020), https://www.nber.org/papers/w26900.

[54] Rebecca Janßen, et al., *supra* n. 9, p.3; Jian Jia, Ginger Zhe Jin & Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment*, NBER Working Paper No. 25248 p.4 (Nov. 2018), https://www.nber.org/papers/w25248.

[55] ANPRM at 73

[56] Daniel Castro & Ashley Johnson, *Maintaining a Light-Touch Approach to Data Protection in the United States*, Information Technology and Innovation Foundation, pp. 8-9 (2022), https://itif.org/publications/2022/08/08/maintaining-a-light-touch-approach-to-data-protection-in-the-united-states/.

[57] *Id* at 3-8; Fred H. Cate & Michael E. Staten, *Protecting Privacy in the New Millenium: THE FALLACY OF "OPT-IN*," University of Chicago pp. 1-4 (2001), https://www.semanticscholar.org/paper/Protecting-Privacy-in-the-New-Millennium%3A-THE-OF-Cate-Staten/2f775d82ef0abd3a740da55c91391f625c23147b.

[58] Canadian Marketing Association, *Privacy Law Pitfalls: Lessons Learned from the European Union*, (2022), p.18-21; Oshrit Aviv, et al., *The Competitive Effects of the GDPR*, p.29-30