ICLE International Center for Law & Economics

Taking Cost-Benefit Analysis Seriously in Consumer-Data Regulation
September 13, 2022
Jonathan Barnett

In its Advance Notice for Proposed Rulemaking (ANPR) on Commercial Surveillance and Data Security, the Federal Trade Commission (FTC) has requested public comment on an unprecedented initiative to promulgate and implement wide-ranging rules concerning the gathering and use of consumer data in digital markets. In this contribution, I will assume, for the sake of argument, that the commission has the legal authority to exercise its purported rulemaking powers for this purpose without a specific legislative mandate (a question as to which I recognize there is great uncertainty, which is further heightened by the fact that Congress is concurrently considered legislation in the same policy area).

In considering whether to use these powers for the purposes of adopting and implementing privacy-related regulations in digital markets, the commission would be required to undertake a rigorous assessment of the expected costs and benefits of any such regulation. Any such cost-benefit analysis must comprise at least two critical elements that are omitted from, or addressed in highly incomplete form in, the ANPR.

The Hippocratic Oath of Regulatory Intervention

There is a longstanding consensus that regulatory intervention is warranted only if a market failure can be identified with reasonable confidence. This principle is especially relevant in the case of the FTC, which is entrusted with preserving competitive markets and, therefore, should be hesitant about intervening in market transactions without a compelling evidentiary basis. As a corollary to this proposition, it is also widely agreed that implementing any intervention to correct a market failure would only be warranted to the extent that such intervention would be reasonably expected to correct any such failure at a net social gain.

This prudent approach tracks the "economic effect" analysis that the commission must apply in the rulemaking process contemplated under the Federal Trade Commission Act and the analysis of "projected benefits and … adverse economic effects" of proposed and final rules contemplated by the commission's rules of practice. Consistent with these requirements, the commission has exhibited a longstanding commitment to thorough cost-benefit analysis. As observed by former Commissioner Julie Brill in 2016, "the FTC conducts its rulemakings with the same level of attention to costs and benefits that is required of other agencies." Former Commissioner Brill also observed that the "FTC combines our broad mandate to protect consumers with a rigorous, empirical approach to enforcement matters."

This demanding, fact-based protocol enhances the likelihood that regulatory interventions result in a net improvement relative to the *status quo*, an uncontroversial goal of any rational public policy. Unfortunately, the ANPR does not make clear that the commission remains committed to this methodology.

Assessing Market Failure in the Use of Consumer Data

To even "get off the ground," any proposed privacy regulation would be required to identify a market failure arising from a particular use of consumer data. This requires a rigorous and comprehensive assessment of the full range of social costs and benefits that can be reasonably attributed to any such practice.

The ANPR's Oversights

In contrast to the approach described by former Commissioner Brill, several elements of the ANPR raise significant doubts concerning the current commission's willingness to assess evidence relevant to the potential necessity of privacy-related regulations in a balanced, rigorous, and comprehensive manner.

First, while the ANPR identifies a plethora of social harms attributable to data-collection practices, it merely acknowledges the possibility that consumers enjoy benefits from such practices "in theory." This skewed perspective is not empirically serious. Focusing almost entirely on the costs of data collection and dismissing as conjecture any possible gains defies market realities, especially given the fact that (as discussed below) those gains are clearly significant and, in some cases, transformative.

Second, the ANPR's choice of the normatively charged term "data surveillance" to encompass all uses of consumer data conveys the impression that all data collection through digital services is surreptitious or coerced, whereas (as discussed below) some users may knowingly provide such data to enable certain data-reliant functionalities.

Third, there is no mention in the ANPR that online providers widely provide users with notices concerning certain uses of consumer data and often require users to select among different levels of data collection.

Fourth, the ANPR unusually relies substantially on news websites and non-peer-reviewed publications in the style of policy briefs or advocacy papers, rather than the empirical social-science research on which the commission has historically made policy determinations.

This apparent indifference to analytical balance is particularly exhibited in the ANPR's failure to address the economic gains generated through the use of consumer data in online markets. As was recognized in a 2014 White House report, many valuable digital services could not function effectively without engaging in some significant level of data collection. The examples are numerous and diverse, including traffic-navigation services that rely on data concerning a user's geographic location (as well as other users' geographic location); personalized ad delivery, which relies on data concerning a user's search history and other

disclosed characteristics; and search services, which rely on the ability to use user data to offer search services at no charge while offering targeted advertisements to paying advertisers.

There are equally clear gains on the "supply" side of the market. Data-collection practices can expand market access by enabling smaller vendors to leverage digital intermediaries to attract consumers that are most likely to purchase those vendors' goods or services. The commission has recognized this point in the past, observing in a 2014 report:

> Data brokers provide the information they compile to clients, who can use it to benefit consumers … [C]onsumers may benefit from increased and innovative product offerings fueled by increased competition from small businesses that are able to connect with consumers that they may not have otherwise been able to reach.

Given the commission's statutory mission under the FTC Act to protect consumers' interests and preserve competitive markets, these observations should be of special relevance.

Data Protection v. Data-Reliant Functionality

Data-reliant services yield social gains by substantially lowering transaction costs and, in the process, enabling services that would not otherwise be feasible, with favorable effects for consumers and vendors. This observation does not exclude the possibility that specific uses of consumer data may constitute a potential market failure that merits regulatory scrutiny and possible intervention (assuming there is sufficient legal authority for the relevant agency to undertake any such intervention). That depends on whether the social costs reasonably attributable to a particular use of consumer data exceed the social gains reasonably attributable to that use. This basic principle seems to be recognized by the ANPR, which states that the commission can only deem a practice "unfair" under the FTC Act if "it causes or is likely to cause substantial injury" *and* "the injury is not outweighed by benefits to consumers or competition."

In implementing this principle, it is important to keep in mind that a market failure could only arise if the costs attributable to any particular use of consumer data are not internalized by the parties to the relevant transaction. This requires showing either that a particular use of consumer data imposes harms on third parties (a plausible scenario in circumstances implicating risks to data security) or consumers are not aware of, or do not adequately assess or foresee, the costs they incur as a result of such use (a plausible scenario in circumstances implicating risks to consumer data). For the sake of brevity, I will focus on the latter scenario.

Many scholars have taken the view that consumers do not meaningfully read privacy notices or consider privacy risks, although the academic literature has also recognized efforts by private entities to develop notice methodologies that can improve consumers' ability to do

so. Even accepting this view, however, it does not necessarily follow (as the ANPR appears to assume) that a more thorough assessment of privacy risks would inevitably lead consumers to elect higher levels of data privacy even where that would degrade functionality or require paying a positive price for certain services. That is a tradeoff that will vary across consumers. It is therefore difficult to predict and easy to get wrong.

As the ANPR indirectly acknowledges in questions 26 and 40, interventions that bar certain uses of consumer data may therefore harm consumers by compelling the modification, positive pricing, or removal from the market of popular data-reliant services. For this reason, some scholars and commentators have favored the informed-consent approach that provides users with the option to bar or limit certain uses of their data. This approach minimizes error costs since it avoids overestimating consumer preferences for privacy. Unlike a flat prohibition of certain uses of consumer data, it also can reflect differences in those preferences across consumers. The ANPR appears to dismiss this concern, asking in question 75 whether certain practices should be made illegal "*irrespective* of whether consumers consent to them" (my emphasis added).

Addressing the still-uncertain body of evidence concerning the tradeoff between privacy protections on the one hand and data-reliant functionalities on the other (as well as the still-unresolved extent to which users can meaningfully make that tradeoff) lies outside the scope of this discussion. However, the critical observation is that any determination of market failure concerning any particular use of consumer data must identify the costs (and specifically, identify non-internalized costs) attributable to any such use and then offset those costs against the gains attributable to that use.

This balancing analysis is critical. As the commission recognized in a 2015 report, it is essential to strike a balance between safeguarding consumer privacy without suppressing the economic gains that arise from data-reliant services that can benefit consumers and vendors alike. This even-handed approach is largely absent from the ANPR—which, as noted above, focuses almost entirely on costs while largely overlooking the gains associated with the uses of consumer data in online markets. This suggests a one-sided approach to privacy regulation that is incompatible with the cost-benefit analysis that the commission recognizes it must follow in the rulemaking process.

Private-Ordering Approaches to Consumer-Data Regulation

Suppose that a rigorous and balanced cost-benefit analysis determines that a particular use of consumer data would likely yield social costs that exceed social gains. It would still remain to be determined whether and howa regulator should intervene to yield a net social gain. As regulators make this determination, it is critical that they consider the full range of possible mechanisms to address a particular market failure in the use of consumer data.

Consistent with this approach, the FTC Act specifically requires that the commission specify in an ANPR "possible regulatory alternatives under consideration," a requirement that is replicated at each subsequent stage of the rulemaking process, as provided in the rules of

practice. The range of alternatives should include the possibility of taking no action, if no feasible intervention can be identified that would likely yield a net gain.

In selecting among those alternatives, it is imperative that the commission consider the possibility of unnecessary or overly burdensome rules that could impede the efficient development and supply of data-reliant services, either degrading the quality or raising the price of those services. In the past, the commission has emphasized this concern, stating in 2011 that "[t]he FTC actively looks for means to reduce burdens while preserving the effectiveness of a rule."

This consideration (which appears to be acknowledged in question 24 of the ANPR) is of special importance to privacy-related regulation, given that the estimated annual costs to the U.S. economy (as calculated by the Information Technology and Innovation Foundation) of compliance with the most extensive proposed forms of privacy-related regulations would exceed $100 billion dollars. Those costs would be especially burdensome for smaller entities, effectively raising entry barriers and reducing competition in online markets (a concern that appears to be acknowledged in question 27 of the ANPR).

Given the exceptional breadth of the rules that the ANPR appears to contemplate—cover an ambitious range of activities that would typically be the subject of a landmark piece of federal legislation, rather than administrative rulemaking—it is not clear that the commission has seriously considered this vital point of concern.

In the event that the FTC does move forward with any of these proposed rulemakings (which would be required to rest on a factually supported finding of market failure), it would confront a range of possible interventions in markets for consumer data. That range is typically viewed as being bounded, on the least-interventionist side, by notice and consent requirements to facilitate informed user choice, and on the most interventionist side, by prohibitions that specifically bar certain uses of consumer data.

This is well-traveled ground within the academic and policy literature and the relative advantages and disadvantages of each regulatory approach are well-known (and differ depending on the type of consumer data and other factors). Within the scope of this contribution, I wish to address an alternative regulatory approach that lies outside this conventional range of policy options.

Bottom-Up v. Top-Down Regulation

Any cost-benefit analysis concerning potential interventions to modify or bar a particular use of consumer data, or to mandate notice-and-consent requirements in connection with any such use, must contemplate not only government-implemented solutions but also market-implemented solutions, including hybrid mechanisms in which government action facilitates or complements market-implemented solutions.

This is not a merely theoretical proposal (and is referenced indirectly in questions 36, 51, and 87 of the ANPR). As I have discussed in previously published research, the U.S.

economy has a long-established record of having adopted, largely without government intervention, collective solutions to the information asymmetries that can threaten the efficient operation of consumer goods and services markets.

Examples abound: Underwriters Laboratories (UL), which establishes product-safety standards in hundreds of markets; large accounting firms, which confirm compliance with Generally Accepted Accounting Principles (GAAP), which are in turn established and updated by the Financial Accounting Standards Board, a private entity subject to oversight by the Securities and Exchange Commission; and intermediaries in other markets, such as consumer credit, business credit, insurance carriers, bond issuers, and content ratings in the entertainment and gaming industries. Collectively, these markets encompass thousands of providers, hundreds of millions of customers, and billions of dollars in value.

A collective solution is often necessary to resolve information asymmetries efficiently because the benefits from establishing an industrywide standard of product or service quality, together with a trusted mechanism for showing compliance with that standard, generates gains that cannot be fully internalized by any single provider.

Jurisdictions outside the United States have tended to address this collective-action problem through the top-down imposition of standards by government mandate and enforcement by regulatory agencies, as illustrated by the jurisdictions referenced by the ANPR that have imposed restrictions on the use of consumer data through direct regulatory intervention. By contrast, the U.S. economy has tended to favor the bottom-up development of voluntary standards, accompanied by certification and audit services, all accomplished by a mix of industry groups and third-party intermediaries. In certain markets, this may be a preferred model to address the information asymmetries between vendors and customers that are the key sources of potential market failure in the use of consumer data.

Privately organized initiatives to set quality standards and monitor compliance benefit the market by supplying a reliable standard that reduces information asymmetries and transaction costs between consumers and vendors. This, in turn, yields economic gains in the form of increased output, since consumers have reduced uncertainty concerning product quality. These quality standards are generally implemented through certification marks (for example, the “UL” certification mark) or ranking mechanisms (for example, consumer-credit or business-credit scores), which induce adoption and compliance through the opportunity to accrue reputational goodwill that, in turn, translates into economic gains.

These market-implemented voluntary mechanisms are a far less costly means to reduce information asymmetries in consumer-goods markets than regulatory interventions, which require significant investments of public funds in rulemaking, detection, investigation, enforcement, and adjudication activities.

Hybrid Policy Approaches

Private-ordering solutions to collective-action failures in markets that suffer from

information asymmetries can sometimes benefit from targeted regulatory action, resulting in a hybrid policy approach. In particular, regulators can sometimes play two supplemental functions in this context.

First, regulators can require that providers in certain markets comply with (or can provide a liability safe harbor for providers that comply with) the quality standards developed by private intermediaries that have developed track records of efficiently establishing those standards and reliably confirming compliance. This mechanism is anticipated by the ANPR, which asks in question 51 whether the commission should "require firms to certify that their commercial surveillance practices meet clear standards concerning collection, use, retention, transfer, or monetization of consumer data" and further asks whether those standards should be set by "the Commission, a third-party organization, or some other entity."

Other regulatory agencies already follow this model. For example, federal and state regulatory agencies in the fields of health care and education rely on accreditation by designated private entities for purposes of assessing compliance with applicable licensing requirements.

Second, regulators can supervise and review the quality standards implemented, adjusted, and enforced by private intermediaries. This is illustrated by the example of securities markets, in which the major exchanges institute and enforce certain governance, disclosure, and reporting requirements for listed companies but are subject to regulatory oversight by the SEC, which must approve all exchange rules and amendments. Similarly, major accounting firms monitor compliance by public companies with GAAP but must register with, and are subject to oversight by, the Public Company Accounting Oversight Board (PCAOB), a nonprofit entity subject to SEC oversight.

These types of hybrid mechanisms shift to private intermediaries most of the costs involved in developing, updating, and enforcing quality standards (in this context, standards for the use of consumer data) and harness private intermediaries' expertise, capacities, and incentives to execute these functions efficiently and rapidly, while using targeted forms of regulatory oversight as a complementary policy tool.

Conclusion

Certain uses of consumer data in digital markets may impose net social harms that can be mitigated through appropriately crafted regulation. Assuming, for the sake of argument, that the commission has the legal power to enact regulation to address such harms (again, a point as to which there is great doubt), any specific steps must be grounded in rigorous and balanced cost-benefit analysis.

As a matter of law and sound public policy, it is imperative that the commission meaningfully consider the full range of reliable evidence to identify any potential market failures in the use of consumer data and how to formulate rules to rectify or mitigate such

failures at a net social gain. Given the extent to which business models in digital environments rely on the use of consumer data, and the substantial value those business models confer on consumers and businesses, the potential "error costs" of regulatory overreach are high. It is therefore critical to engage in a thorough balancing of costs and gains concerning any such use.

Privacy regulation is a complex and economically consequential policy area that demands careful diagnosis and targeted remedies grounded in analysis and evidence, rather than sweeping interventions accompanied by rhetoric and anecdote.

View Article