NetChoice Comment for the Record:

Federal Trade Commission (FTC)

Request for Comments on

Advance Notice of Proposed Rulemaking on

Commercial Surveillance and Data Security,

November 15, 2022

NetChoice is a trade association of leading internet businesses that promotes the value, convenience, and choice that internet business models provide to American consumers. Our mission is to make the internet safe for free enterprise and free expression. We also work to promote the integrity and availability of the internet on a global stage and are engaged on issues in the states, in Washington, D.C., and in international internet governance organizations.

Data privacy and security is the top tech policy concern for many American voters.[1] The federal framework around data privacy and security will be critically important to consumers and innovators in a wide array of industries. It also, however, remains critically important that the approach to this issue balances all the potential tradeoffs and is thoroughly considered through the appropriate processes and not a regulatory overreach. Data privacy and security rules could impact almost every aspect of the American economy and the day-to-day life of American consumers.

[1] Carl Szabo, "New National Poll: Americans Oppose Antitrust Regulations That Harm American Tech," NetChoice. January 20, 2022. https://netchoice.org/new-national-poll-americans-oppose-antitrust-regulations-that-harm-american-tech/ .

1. Introduction

The Federal Trade Commission (FTC) is seeking comments regarding the "prevalence of commercial surveillance practices and data security practices that harm consumers." While we welcome the opportunity to provide feedback on the important issue of data privacy and security, we also must highlight concerns that the agency has overstepped its regulatory authority. The nature and scope of the ANPR exceeds the FTC's limited Section 18 rulemaking authority. The FTC fails to meet the criteria necessary as it does demonstrate the practices targeted are "unfair," meaning that they are prevalent, unavoidable by consumers, and harms that result are not outweighed by countervailing benefits. In fact, many of the practices identified have substantial consumer benefits that provide better experiences at lower costs in a range of industries from agriculture to retail to technology.

Based on our previous work and expertise, we highlight the following overarching concerns regarding the agency's proposal to engage in this process:

- The importance of the agency receiving proper Congressional authority before expanding its actions in this critical area;
- The problematic framing of the FTC's actions around "consumer surveillance" that could restrict and malign beneficial and benign data practice;
- The FTC should use its limited resources to focus on data privacy concerns that are clearly within its mission rather than intervening in every facet of the American economy;
- The ability of existing laws to address some of the highlighted underlying concerns about potential harms;
- The need for any privacy rules to be firmly grounded in the concept of consumer harm.

It is especially critical that FTC not engage in rulemaking at a time when Congress is close to acting on data privacy. Particularly, considering the recent Supreme Court

decision in *West Virginia v. EPA*[2] regarding the "Major Questions" doctrine, any rulemaking not tied to a specific congressional grant of authority will likely face legal challenges to the agency's authority and procedures. With legislation currently pending in Congress, the agency must wait for Congress to give guidance and authority around this issue.

2. "Commercial Surveillance," lax data security measures, and consumer harm

Over the years, companies have taken many steps to empower consumers to understand how their data is used and to choose settings that align with their privacy preferences. The Commission should not assume that one size fits all, either in the options companies are able to offer consumers or in consumers preferences. After all, since companies may interact with consumers differently such as through an app, website, or physical store, how they present consumers with options for privacy will differ. Some of the growing number of tools available to consumers include prompts for privacy and security checkups and alerts about compromised data or passwords. Additionally, some companies have even highlighted their use of less data or investing in features to meet the specific needs of more privacy-sensitive consumers. Similarly, many companies increasingly nudge consumers to use security best practices such as multi-factor authentication.[3]

Consumer preferences often vary depending on how sensitive they consider the data. Existing privacy laws have been designed in response to this by creating specific standards for processing of information that is more likely to lead to irreversible or catastrophic harm if compromised such as financial information, medical records, protected health information, and children's information.[4] However,

---

[2] *West Virginia et al. vs. Environmental Protection Agency et al.*, 597 U.S. ____ (2022).

[3] Derek Rodenhausen, et al., "Consumers Want Privacy. Marketers Can Deliver." Boston Consulting Group, January 21, 2022. https://www.bcg.com/publications/2022/consumers-want-data-privacy-and-marketers-can-deliver.

[4] Alan McQuinn, "Understanding Data Privacy," Real Clear Policy, October 25, 2018, https://www.realclearpolicy.com/articles/2018/10/25/understanding_data_privacy_110877.html.

even in these cases where it is widely agreed the information is highly sensitive, increased regulation can make it difficult both for consumers and innovators to come up with new solutions such as more portable patient records. The Commission should not import a one-size-fits-all approach that treats all data as highly sensitive and should be wary of the consequences of engaging in broad regulation of categories that may contain data of a mixed degree of use sensitivity such as biometrics.

Regulations should also exempt from processing restrictions processing of personal information for purposes of fraud prevention, anti-money laundering processes, screening, or to otherwise comply with legal obligations.

Much of the Advance Notice of Proposed Rulemaking (ANPR) presumes that data collection or usage is inherently harmful. In reality, data collection already has many benefits to consumers from providing better commuter routes to providing us with free services that were once or would be costly. And for the bad actors who truly engage in consumer harm, the FTC already has the authority to go after those individuals as it has done in the past with cases against those who had inadequate security practices and were subject to data breaches and those who engaged in deceptive data practices. The agency should not equate beneficial data practices and over-regulate the data environment that benefits many consumers in response to bad actors.

Privacy is an area where consumers may have stated preferences that differ from their revealed preferences. The revealed preferences show that most consumers prefer to continue using services that use their data rather than pay for an alternative version, should the business model change.[5] Instead of focusing on dictating a specific formula around services and limiting the use of data to respond

[5] Tracey Lien and David Pierson, "Would you pay for an ad-free Facebook?" Los Angeles Times, April 13, 2018. https://www.latimes.com/business/technology/la-fi-tn-facebook-paid-version-20180413-story.html .

to the most privacy-sensitive consumers, the agency should maintain its current approach that focuses on concrete harms and deception. This authority should only be used when there are clear harms that meet existing legal standards rather than for subjective preferences around the idea of privacy. The agency should avoid defining harms that are not quantifiable or measurable as it will inevitably lead to removing a number of beneficial uses and create confusion for consumers and innovators. Instead, it should use its limited resources to focus on data privacy concerns that are clearly within its mission rather than expanding to intervene in every facet of the American economy. Enforcement should focus on those clear cases of bad actors and actual consumer harm, rather than create a burdensome regulatory regime that presumes innovative data uses are guilty until proven innocent.

The Commission has been a zealous enforcer when it comes to exercising its existing authority and should not overstep such authority without a Congressional grant to do so. For example, the FTC has pursued significant cases where there was clear consumer harm like its case against Ashley Madison[6] and where previous consent decrees have been violated as in the Cambridge Analytica scandal[7]. Where consumer harm is clear and appropriate legal standards are met, the FTC has successfully pursued action around data privacy and cybersecurity within the bounds of its authority. It should not *sua sponte* expand its authority without a grant from Congress.

The FTC should focus on those harms for which quantifiable relief can be recovered within the scope of its existing authority. Consumers want to know their data is

---

[6] Morgan Sharp and Diane Bartz, "Ashley Madison owner to pay $1.66 million to settle FTC case," Reuters, December 16, 2016. https://www.reuters.com/article/us-ashleymadison-cyber-settlement/ashley-madison-owner-to-pay-1-66-million-to-settle-ftc-case-idUSKBN14325X.

[7] Carrie Mihalcik, "Federal court approves $5B Facebook settlement with FTC over Cambridge Analytica," CNet, April 24, 2020. https://www.cnet.com/tech/mobile/federal-court-approves-facebook-settlement-with-ftc-over-cambridge-analytica/.

secure. Therefore, there is an incentive from both economic and reputational risk to engage in reasonable data practices. The FTC's ANPR questions often conflate lax data security and surveillance with personal privacy preferences, and this problematically risks maligning beneficial and benign practices with those of bad actors. It is important that the agency make clear the distinctions between its intended actions on data security and data privacy.

Rather than creating new rules without a clear grant of authority from Congress, the Commission should consider how it can appropriately use its existing tools to go after bad actors. Creating a new, comprehensive set of regulation that does not clearly distinguish between benign, beneficial data use and malicious data practices may deter innovation and prohibit the practices and services that benefit consumers.

3. Protecting Kids and Teenagers Online

Many parents and policymakers are concerned about how young people use certain online services. This is not unusual when it comes to the development of new technologies. A variety of tools exist to empower parents and families to make informed choices about their child's use of technology, have conversations with their children about technology, and help keep their kids from harmful content online.[8] These tools include both native controls like age-gating certain content, time limits within apps, and additional services for blocking or filtering certain types of content. Policymakers like the FTC seeking to protect children, however, must be cautious about wading into family decisions and the consequences their choices could have for adults, innovation, and the young people they seek to protect.

In some scenarios, the FTC already has existing authority under the Children's Online Privacy Protection Act (COPPA). However, it must be careful to not engage in overzealous regulation that would limit the availability of valuable technology for

[8] *See* Family Online Safety Institute. "Good digital parenting." https://www.fosi.org/good-digital-parenting.

young people and families. COPPA understands that young people may be more vulnerable and need adult supervision to learn how to navigate technology safely, but it also recognizes that teenagers have different expectations, needs, and knowledge than younger children.

The FTC must be cautious not to overstep its existing authority granted by COPPA. Congress has the power to amend COPPA, not the FTC. In any considerations about potential further regulation, policymakers should consider the tradeoffs between beneficial opportunities and innovations for young people and any risks. For example, erasure raises speech concerns and safety risks for deleting information about predatory behavior.[9]

When it comes to any potential rulemaking, the Commission should not broaden the scope of its authority especially without authorization from Congress. Changes to COPPA to cover additional types of content or raise the age limit could have much broader implications beyond privacy or the data of young people. For example, the suggestion of putting limitations on general use services raises concerns for the impact on adults' rights and speech and potentially creates constitutional concerns. Additionally, there is a reason why distinctions have been made between children under 13 and teenagers. For example, an older teenager may need to use the internet for access to sensitive information such as religion, health, sexuality, and sexual health for which they may be uncomfortable seeking parental approval.

COPPA limitations on children's information may raise the cost of services and limit the availability of free or advertising supported products and services. Putting additional limitations on data could further hinder the development of technology for children by raising the costs to both innovators and families. The alternative

---

[9] Jennifer Huddleston, "Want to Keep Kids Safe Online? Don't Just 'Do Something.'" Real Clear Policy. November 16, 2021. https://www.realclearpolicy.com/articles/2021/11/16/want_to_keep_kids_safe_online_dont_just_do_something_803758.html.

could also increase costs of certain products such as learning apps, increasing the digital divide and other education gaps by decreasing the availability of free resources to families.

Almost every new technology has brought with it new fears about the impact on the next generation. Current fears around social media and teenage mental health are no different.[10] There are still mixed findings and no scientific consensus connecting such concerns, and regulators should not rush to eliminate beneficial uses without understanding the full relationship on such complex issues.[11] Existing laws including COPPA already recognize the difference in young people's experience of advertising and ability to consent to data collection in relation to their unique vulnerability. Policymakers should ensure any further restrictions are backed up by a thorough understanding of the relationship between technology and advertising. This includes both opportunities to engage in education for parents about the tools available to them to understand their child's online activities or other uses of their child's data. Other tools policymakers may consider instead of rulemaking would be Commissioned studies to better understand and gather thorough data the potential relationship to these concerns and ensure any proposals are in response to documented harm and not merely maligning technology's use by young people.[12] Should other laws covering information like health or banking not apply to those under 13 or 18, then Congress should clarify their application and relationship to COPPA and other protections of minors. The FTC should only act as enforcer or create rules where it is clearly authorized to do so.

---

[10] *See generally,* Pessimist archive, https://pessimistsarchive.org/ .

[11] Andrea K. McDaniels, "Research offers mixed messages on the impact of social media on adolescent emotional health," The Baltimore Sun, June 2, 2017, https://www.baltimoresun.com/health/bs-hs-social-media-teens-20170526-story.html.

[12] *See*, *e.g.*, U.S. Congress, Senate, *Children and Media Research Advancement Act (CAMRA Act),* 115th Congress, 2nd Session, https://www.markey.senate.gov/imo/media/doc/CAMRA%20Act.pdf.

Rather than seeking to impose additional regulations, policymakers such as the Commission should focus on informing parents about the tools available to address their concerns about their children's online behavior and how to have difficult conversations with their children about technology use and content.

4. Cost-Benefit Considerations

While privacy is a value, it does not exist in a vacuum. In considering any actions, the Commission must also consider the potential tradeoffs involved including the impact the burdens of regulation might have on the costs of products to consumers, the ability to innovate and provide better privacy options, and the impact on small and mid-size players' ability to remain competitive.

With this in mind, the Commission must consider the costs of compliance relative to improved protection as seen from CCPA and GDPR. For example, GDPR has seen less app development in the European market and a growth in the market share of large players as well as the at least initial exit of some businesses ranging from newspapers to video games in the online market.[13] California's own economic analysis estimates that CCPA (now CPRA) compliance costs would be up to $55 billion.[14] These costs will grow significantly as out-of-state businesses will also be impacted and a growing state patchwork will further raise costs.[15] In addition to the costs to businesses, such regulations will increase costs for consumers and could negatively the income of online content creators. The Commission must not merely

---

[13] Rebecca Janßen, et al., *GDPR and the Lost Generation of Innovative Apps.* National Bureau of Economic Research. May 2022. https://www.nber.org/papers/w30028.

[14] Lauren Feiner, "California's new privacy law could cost companies a total of $55 billion to get in compliance," CNBC, Revised on October 8, 2019. https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html .

[15] Information Technology & Innovation Foundation. "50-State Patchwork of Privacy Laws Could Cost $1 Trillion More Than a Single Federal Law, New ITIF Report Finds" https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/ .

consider the potential costs on individual businesses but how such regulation would prove costly to an entire business ecosystem, raising prices for consumers and advertisers and reducing the return for small businesses and content creators.

When it comes to the potential burden, a federal standard is preferable to a state approach in overcoming a patchwork. However, this must come from Congress or with a specific delegation of authority, not just *sua sponte* from the FTC. As seen in the initial aftermath of GDPR, an inappropriate level of regulation could further reduce the ability of small businesses to compete. It could also entrench existing practices even if better ones would have emerged in the marketplace. While the FTC must carefully consider all costs, it should only engage in formal cost-benefit analysis or rulemaking as its existing authority grants under specific laws such as COPPA.

While it is clear that we have started to see fracturing of the internet across national, and now state lines, and the time has come for establishment of a nationwide standard for privacy online, the development of such a standard falls to Congress not the FTC until Congress expressly delegates that authority to the FTC. This standard should be a better way to protect all — not relying on failed approaches abroad or domestically.

In considering a federal standard, the first step is for Congress to create federal legislation that preempts state privacy laws. The internet has no borders, and businesses in one state should not be subjected to the whims of a different state's legislature. Much in the way the U.S. led in implementing COPPA[16] and Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM),[17] Congress should enact federal privacy legislation that creates a ceiling on privacy protections and creates certainty for consumers and businesses alike. Such an approach must be buttressed with clear definitions of who and what are covered.

[16] 15 U.S.C. § 6501, *et sec.*

[17] 15 U.S.C. § 103.

Then, Congress should advance this better approach on privacy internationally. This would include integration of the American privacy approach in trade agreements, supporting the continued benefits of data and innovation led by America's global leaders in information technology and a plethora of other industries. This approach should also establish that compliance with US privacy laws is adequate for a foreign country's privacy laws.

5. Potential Commission Action on Harmful Commercial Surveillance or Data Security Practices

As mentioned above, the FTC has not been delegated authority to engage in data privacy rulemaking. In fact, at this time, Congress is currently debating potential data privacy legislation and has engaged in consideration of the appropriate agency delegations. If the FTC were to act prior to such a delegation, it would certainly face legal challenges particularly in the wake of *West Virginia v. EPA*.[18]

This rulemaking is not the first overreach of FTC authority. Past overreach by the agency led it to be subjected to further restraints in rulemaking by Congress in the 1980s. We worry that if the FTC does not cease its overreaching, it's putting itself on a collision course with Congress and the courts.

Collection, Use, Retention, and Transfer of Consumer Data

Biometric data from fingerprints to voice authentication can be useful for improving security practices and consumer experiences for everything from boarding an airplane and ordering food to securing floors of office buildings or providing a layer of security against bad actors for individuals, houses of worship, and childcare centers. As has already been seen in Illinois after passage of the Illinois Biometric Information Privacy Act, over-regulation and litigation could deter innovation and result in a less secure option for consumers. As stated in earlier sections, the Commission should avoid wrongly misclassifying beneficial and benign data

[18] *West Virginia et al. vs. Environmental Protection Agency et al.*, 597 U.S. ____ (2022).

practices as “commercial surveillance” and focus on specific harms to consumers within the scope of their authority.

To the extent the Commission promulgates rules on this topic, rules should require affirmative and informed consent (including written, verbal, or other clear, unambiguous acts) for collection of biometric data, with a few guardrails.

(1) Consent should be required only when the controller stores the data, and not when collection is for an ephemeral use and then immediately purged (for example, to check if someone is enrolled in a service) or when the data is solely stored on user devices. Consent should be required only at the stage where the consumer enrolls in a service—the consumer should not then be required to consent every time the collected biometric identifier is used to perform the service, such as to authenticate identity.

(2) Avoid consent requirements that would result in eliminating products and services that generate substantial consumer benefit, with minimal risk of unfair or deceptive consequences. For instance, consumers routinely use online photo album features that automatically sort contacts based on facial geometry. A broad consent rule would wipe out this feature since it would be impossible to obtain consent from all of these contacts.

(3) Exempt consent for security and emergency situations. For instance, stores should have the ability to screen for known criminals or shoplifters, who would not otherwise consent. Facial recognition technology should also be permitted to screen for a missing person, who is not available to provide consent.

The scope of regulations should be limited to biometric identifiers, i.e., data generated by automatic measurements of an individual's biological characteristics that is used to identify a specific individual. It should not cover merely the collection of data from which biometric identifiers may be extracted, such as a physical or

digital photograph, a video or audio recording or data generated therefrom unless such data is generated to identify a specific person.

Similarly, the FTC should not equate ad-supported services and the current advertising ecosystem with malicious and malevolent behaviors by grouping them together as “commercial surveillance”. Current data practices have lowered the cost of advertising and better enabled small businesses to reach customers while also providing consumers with free services. If companies were unable to continue such practices, business models would have to pass along costs directly to consumers, and advertisers would have fewer options to reach their consumers. The leftover advertising available would then be at a higher cost. The result would harm small businesses and consumers already facing increasing prices from inflation. For those consumers who do not find this to be a beneficial practice, existing products already notify them of their data options, whether it be through notices of app tracking, cookie alerts, privacy checkups, or specifically targeted privacy products such as ad-blockers and VPNs.

The FTC should avoid dictating specific practices such as data minimization. Data minimization may not work in all cases, and it may be difficult to determine what data is useful in advance. Instead, consumers should be empowered to make informed decisions around which services they trust with which data, and the Commission should focus on harm, not mere collection. The Commission should not engage in product design and instead should continue to address issues of harm. Similarly, the Commission should not expand its authority to those specific concerns such as banking and employment that are already delegated to other agencies. Existing law around discrimination and regulated industries likely better covers these concerns and addresses them in a way proportionate to the harm. The agencies tasked with these issues have greater expertise in the ways to understand harms, business practices, and tradeoffs associated with the industry practices and harms they are tasked with.

In all of these cases and in approaching the question of data privacy more generally,

the Commission should focus on consumer harm and not vilify collection or benign uses of data.

Automated Decision-Making Systems

Automated decision-making systems (ADS), algorithms, and artificial intelligence (AI) are tools and as with any tool they can be used for various purposes with various intentions. The FTC does not place strict restrictions on computers because they might be abused by bad actors, and similarly, it should consider caution when regulating algorithms that on their own cause no harm. Many of the concerns about abuse are best addressed by existing laws such as those around discrimination and credit and provide appropriate agencies with redress for those who may engage in problematic, harmful, or predatory uses of this technology. Still, these technologies remain as tools that can be useful for many practices throughout many industries and could be used to combat existing implicit or explicit bias in society.[19] It would be far easier to respond and correct algorithms should they be found to disproportionately impact a group than the many years it may take human beings to make similar social changes among peers.

As mentioned, existing law addresses many concerns around issues such as discrimination. Heavy-handed regulation would be burdensome on both the existing tools relied on by businesses and consumers and the development of new tools. For instance, algorithms are employed in many ways and constantly evolve that requiring certification would disrupt many of the tools consumers rely on. And these uses remain subject to existing federal, state, and common law. On June 8, 2022, CFPB Director and former FTC commissioner Rohit Chopra reiterated this point when he said, "Companies are not absolved of their legal responsibilities when they let a black-box model make lending decisions." [20]

---

[19] Jennifer Huddleston, "AI Is a Tool, Not a Villain," Real Clear Policy, October 3, 2022, https://www.realclearpolicy.com/2022/10/03/ai_is_a_tool_not_a_villain_856760.html .

[20] Consumer Financial Protection Bureau. "CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms," May 26, 2022. https://www.consumerfinance.gov

ADS, algorithms, and AI have been increasingly a part of consumers' lives from virtual assistants on their phones to traffic apps that tell them the quickest way to get to work. These tools allow many products and services to remember and incorporate consumer preferences. In some cases, algorithms can provide quicker and more objective responses and allow faster reaction times to consumer complaints.

If the FTC were to begin requiring advanced approval for the use of these tools, innovation and opportunities would move much more slowly. But even more concerning is that consumers' experiences would be slower, less responsive, less personalized, and overall less enjoyable. The FTC should not create new rules given that most of the harms they are concerned about are already covered by existing law, and there has not been a clear Congressional mandate to do so.

Finally, in this section, we turn to the legal question the Commission raises regarding the First Amendment, Section 230, ADS, and algorithms. As the Supreme Court has explained, "whatever the challenges of applying the Constitution to ever-advancing technology," the First Amendment's commands do not change when a "new and different medium for communication appears."[21]
The First Amendment leaves little to no room for the Commission to regulate personalized services or targeted advertising. First, the First Amendment protects computer code,[22] including algorithms used to display third-party content to specific

---

/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/.

[21] *Brown v. Entertainment Merchants Assn.*, 564 U.S. 786, 790 (2011) (internal quotation marks omitted).

[22] *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132, 1141 (9th Cir. 1999) (concluding that "encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes").

users[23]. Second, the First Amendment protects editorial discretion from government interference, including from so-called "conduct" regulations.[24] And third, the First Amendment protects commercial speech.[25]

To start, the First Amendment protects computer codes like algorithms because, among other things, they communicate information.[26] Indeed, a "central purpose" of many codes including search engines, "is to retrieve relevant information from the vast universe of data" and then "to organize it in a way that would be most helpful" to the user.[27] Personalized services and targeted advertising both share that central purpose and communicate information.

In presenting information to users, codes "inevitably make editorial judgments about what information (or kinds of information) to include in the results and how and where to display that information."[28] After all, "algorithms themselves [are] written by human beings" and thus "inherently incorporate" the business's "judgments about what material users are most likely to find" relevant to them.[29]

---

[23] *E-ventures Worldwide, LLC v. Google, Inc.*, 188 F. Supp. 3d 1265, 1274 (M.D. Fla. 2016); *Zhang v. Baidu.com Inc.*, 10 F. Supp. 3d 433, 438- 39 (S.D.N.Y. 2014); *Search King, Inc. v. Google Tech., Inc.*, No. CIV-02-1457-M, 2003 WL 21464568, at *4-5 (W.D. Okla. 2003).

[24] *See, e.g.*, *NetChoice v. Moody*, 34 F.4th 1196, 1230-31 (11th Cir. 2022).

[25] *Virginia State Bd. of Pharm. v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 762 (1976).

[26] *Zhang*, 10 F. Supp. 3d at 437-38.

[27] *See id*. at 438.

[28] *See id.* (citing Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 Yale J.L. & Tech. 188, 192 (2006)).

[29] *See id.* (internal quotation marks omitted) (quoting Eugene Volokh & Donald M. Falk, *GOOGLE: First Amendment Protection for Search Engine Results*, 8 J.L. Econ. & Pol'y 883, 888-90 (2012)).

That includes judgments about which content to display, when, where, and to whom. Those judgments needn't even produce a coherent or unified message either: "A private speaker does not forfeit constitutional protection simply by combining multifarious voices, or by failing to edit their themes to isolate an exact message."[30]

Even if personalized services and targeted content were considered "commercial speech," the First Amendment would still prohibit the Commission from regulating the "inputs" and "outputs" of codes. In other words, even if the Commission promulgated rules that narrowly targeted only services or advertisements that propose a commercial transaction, the First Amendment still prohibits the government from regulating the "final" product (information shown to users) and the editorial judgments that led to the final product.

Because an algorithm's inputs and outputs are intertwined, the Commission may not infringe on an algorithm's constitutionally protected inputs without infringing the algorithm's constitutionally protected outputs and vice versa.

Discrimination Based on Protected Categories

As mentioned in the above section, many of the expressed concerns about discrimination are already covered by existing law and could be handled by the appropriate agencies such as the EEOC, CFPB, and FHA that are tasked with enforcing these laws. The Commission should focus on the enforcement of its existing laws and allow the appropriate agencies to engage in any necessary enforcement of discrimination laws. The development of a new technology does not create an opportunity for the FTC to declare itself the enforcement agency for laws within other agencies' purview nor does it give it a grant of authority to engage in rulemaking without congressional authorization.

[30] *Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp.*, 515 U.S 557, 569-70 (1995).

In fact, the Commission's involvement and suggestions in this notice could also prevent the highlighting of certain communities such as black-owned businesses or women authors.

The Commission should focus on enforcing only legal, cognizable harms as currently established by law and its existing authority. The Commission is not authorized to create new, protected classes when it comes to legal enforcement.

Consumer Consent

As mentioned, multiple times, the Commission's use of the term "consumer surveillance" is problematic and wrongly equates the beneficial use of data and the current advertising ecosystem with malicious actions. Data has generally improved a wide range of consumer experiences online and offline. As a result, the ways businesses and consumers engage and the manners in which consumers' consent is obtained may vary broadly. Consumers have a wide range of preferences when it comes to their privacy around different types of data and should be trusted to act on those.[31] Education, not regulation, is a more appropriate response to concerns about consumer consent. However, the Commission should not presume that those whose preferences are not privacy-centric have somehow been misled. When it comes to consumer consent, the Commission should continue its existing approach to privacy focusing on consumer harm and deception.

Any regulations around consent should allow flexibility in the form that consent takes, in order to facilitate customer experiences across a range of devices and services. The regulations should not prescribe required forms of consent. This is particularly important where certain forms of consent might not be compatible across technologies. For instance, some devices that are voice activated do not have

[31] Alec Stapp, "Against Privacy Fundamentalism in the United States," Niskanen Center, November 19, 2018. https://www.niskanencenter.org/against-privacy-fundamentalism-in-the-united-states/ .

a physical interface and so consumers should have the option to provide verbal consent. This approach avoids burdening the consumers with complicated multi-step consent processes.

Depending on the service, there are a growing range of options and nudges to consumers to ensure their privacy settings meet their preferences. Even after signing up, a growing number of services already provide consumers with options around their data collection and privacy and options to review it whether it is via a privacy checkup, a notification that an app is accessing certain information, or notifications of changes to a privacy policy. Consumers already have choice and are able to exercise such choices in the products they select. In fact, due to consumer demands, not government regulation, many products distinguish themselves to consumers by their privacy and security features. The FTC should focus on harm, not on playing product designer.

If there are opportunities to improve consumers' understanding, it should be done through education rather than regulation. This may include information on frauds and scams and how to access privacy options particularly for those less accustomed to technology. The FTC and companies already engage in many of these educational practices, but as always, this educational material needs to be updated as new threats arise.

If companies are clearly engaged in deceptive practices around their privacy practices, the Commission already has the authority to act and has done so in the past. It does not need new rules to do so.

Notice, Transparency, and Disclosure

Providing consumers with information about data policies or other practices can be a good choice for companies in response to consumer demands or to distinguish a company. But government mandates of such practices raise constitutional concerns under the First Amendment. Government-compelled disclosures could also provide

bad actors with a roadmap to escape detection. In fact, decisions about what policies to disclose, in what depth, and by which means vary widely depending on the way the service interacts with users.

The FTC should avoid mandating the specifics of a requirement as it will not work equally for all products and will very likely veer into compelled speech, raising constitutional concerns under the First Amendment. As have been seen in NetChoice's ongoing lawsuits against Florida and Texas, state content moderation laws, including transparency requirements," threaten to require platforms to reveal trade secrets and other nonpublic, competitively sensitive information about how their algorithms and platforms operate. Above all, these detailed requirements interfere with, and chill the exercise of, platforms' editorial discretion."[32] The FTC will likely face similar legal challenges if it dictates disclosure requirements in the name of privacy.

Such concerns are more likely to arise if the FTC is seeking to dictate the nature, style, and content of the disclosure. For example, plain language requirements set an arbitrary definition of what and how a platform must disclose that may not appropriately reflect the use of data as seen in the California proposal of a "do not sell" button.

Positively, many companies already provide privacy disclosure information voluntarily. But because those disclosures are voluntary and made according to the companies' own editorial discretion, they raise none of the same concerns as government-compelled disclosures. In fact, they know how best to balance disclosure with cautiousness about both proprietary information and the sensitivity of information that could be used to find loopholes in the system by bad actors.

[32] Complaint for NetChoice et al v. Paxton, 1:21-cv-00840, Western District of Texas https://netchoice.org/wp-content/uploads/2021/09/1-main.pdf.

Remedies

The FTC should not establish new remedies without express congressional authorization to do so. This is especially true considering recent Supreme Court decisions on the "Major Questions Doctrine." While the FTC has the limited authority to define with specificity what constitutes an unfair or deceptive act or practice, this ANPR covers topics well beyond such practices. Without a clear grant of statutory authority from Congress to issue broad sweeping rules related to privacy and data use, the FTC arguably does not have the authority to undertake this endeavor. In fact, Congress is considering data privacy bills and has not yet granted the FTC with the authority to enact broad rules on this topic. Rather than establishing new remedies or rules to enforce, the FTC should use its limited resources to focus on data privacy concerns that are clearly within its mission. Its remedies and enforcement should continue to focus on those clear cases of bad actors and actual consumer harm, rather than create a burdensome regulatory regime that presumes innovative uses of data are guilty until proven innocent.

Obsolescence

One of the advantages to the light touch approach is that it has been better able to evolve with changing technologies than a more restrictive and precautionary approach. In what has often been termed the "pacing problem," technology will move faster than rules can evolve.[33] Restrictive regulations can therefore prevent improved innovations in critical spaces including privacy and data security by limiting the ability to try new and different solutions that fail to meet existing standards. The FTC's current, light touch approach allows innovators to meet consumer demands while still providing a response in the case consumers are harmed. This approach is far better suited to support the wide array of data uses in a wide range of industries and to encourage developments in privacy and security to

[33] *See* Adam Thierer, "The Pacing Problem and the Future of Technology Regulation," Mercatus Institute, August 8, 2018. https://www.mercatus.org/bridge/commentary/pacing-problem-and-future-technology-regulation.

meet consumer needs. Rigid rules would be unlikely to keep pace with the growing and beneficial uses of data in a wide range of industries.

6. Conclusion

While we appreciate the opportunity to provide feedback during the ANPR process, we would like to again highlight our significant concerns about the lack of congressional delegation and concerns that the FTC has reached a foregone conclusion about its desired outcome make this proposed policy change a further example of the agency's overreach. In addition to these concerns, the FTC in many cases seems to have come to a foregone conclusion to demonize common business practices that have benefitted American consumers. We ask that the FTC continue to follow the approach to regulation that has allowed American innovation to flourish and consumers to have more, better, and lower cost options than ever before. The FTC's best response is to focus its limited resources on those consumer harms occurring within its existing authority as it has done on data privacy and security in the past.