



# University of Pittsburgh

Kenneth P. Dietrich School of Arts and Sciences  
Department of Communication

1433 Cathedral of Learning  
4200 Fifth Avenue  
Pittsburgh, PA 15260  
412-624-6567  
Fax: 412-624-1878  
www.comm.pitt.edu

## *Evidence-Based Commentary on Federal Trade Commission Commercial Surveillance Rulemaking*

### **Individual Student Responses to FTC's Call for Public Comments**

University of Pittsburgh undergraduate student research collaborative

Corresponding authors:

Austin Hogeboom (adh90@pitt.edu) & Alyssa Morales (alm489@pitt.edu)

November 2022

### Contents

(click to jump to selected content when in Word format)

<i>Background</i> .....	2
<i>Critical Approach</i> .....	2
<i>Comment Texts</i> .....	4
Comment Submitted by William Allen .....	4
Comment Submitted by Anonymous .....	6
Comment Submitted by Kathryn Chang .....	8
Comment Submitted by Colin Dyer .....	10
Comment Submitted by Austin Hogeboom .....	12
Comment Submitted by Lukas Kim.....	14
Comment Submitted by Kamryn Kostelnik .....	15
Comment Submitted by Alyssa Morales.....	17
Comment Submitted by Marlo Postufka .....	19
<i>Appendices</i> .....	21
Appendix 1: FTC Public Forum Scouting Assignment.....	21
Appendix 2: FTC Public Forum Jamboard Assignment .....	22
Appendix 3: Jamboard Assignment Work Product Example .....	23
Appendix 4: Adjacent Curriculum Description .....	24
Appendix 5: Optional Assignment Grading Rubric .....	25
Appendix 6: Optional Assignment Workflow Chart .....	26

## Background

The United States Federal Trade Commission (FTC) is a federal government agency with a [mission](#) of "protecting the public from deceptive or unfair business practices and from unfair methods of competition through law enforcement, advocacy, research, and education."<sup>1</sup> On August 22, 2022, the FTC announced [advance notice of proposed rulemaking](#) (ANPR) on commercial surveillance, defined as "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information."<sup>2</sup> In addition to signaling that the agency is considering adoption of federal rules on commercial surveillance, this ANPR invited public participation in the rulemaking process (see Fig. 1).



Figure 1. FTC advanced notice of potential rulemaking on commercial surveillance, August 22, 2022.

## Critical Approach

This document carries individual student comments officially submitted to the FTC in response to the agency's ANPR comment call. Highlighting significance of the student initiatives, FTC Commissioner Alvaro Bedoya [stressed recently](#) regarding the ANPR: "You do not need to be an expert to comment on this process, and in fact, I would urge you that if you know there's a thought in the back of your mind, 'I think this is interesting, but I'm only in high school, I'm only a college student, I'm only a law student, I'm only an engineering student,' and you have something to say, please, by all means, comment and say it."<sup>3</sup>

Responding to commissioner Bedoya's call, student comments were developed as part of an optional assignment in "Evidence," an undergraduate communication course at the University

---

<sup>1</sup> See United States Federal Trade Commission, "About the FTC," <https://www.ftc.gov/about-ftc>

<sup>2</sup> United States Federal Trade Commission, "Trade Regulation Rule on Commercial Surveillance and Data Security," Proposed Rule. August 22, 2022, <https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security>

<sup>3</sup> Alvaro Bedoya, statement, Commercial Surveillance and Data Security Public Forum. September 8, 2022. U.S. Federal Trade Commission, [https://www.ftc.gov/system/files/ftc\\_gov/pdf/CommercialSurveillanceandDataSecurityRulemakingTranscript09.08.2022.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/CommercialSurveillanceandDataSecurityRulemakingTranscript09.08.2022.pdf)

of Pittsburgh. The following timeline conveys assignment sequencing and details on how a collaborative undergraduate student research effort supported drafting and refinement of submitted comments compiled herein.

- **August 22, 2022:** FTC provided [advanced notice of proposed rulemaking](#) on commercial surveillance, announcing a public forum and opening of a 60-day public comment window (subsequently extended by one month).<sup>4</sup>
- **September 8, 2022:** FTC hosted a [public forum](#) regarding its ANPR on commercial surveillance and data security practices that harm consumers and competition. Students scouted the forum, classifying and sorting contributions into six broad areas: harms, AI, consent/transparency, minors, advertising, and discrimination (see Appendix 1). Findings were shared and discussed during a September 13, 2022 class exercise linking in-person deliberation with Google Jamboard (see Appendix 2-3).
- **September 13-October 18, 2022:** Draft comment writing period for 21 students opting into assignment (see Appendices 4-5), including online peer review via Canvas.
- **October 18, 2022:** Students completing the optional assignment began submitting comments to FTC.
- **November 7-9, 2022:** Individual student comments published in the *Federal Register*, documenting contributions to the FTC call for public comment.
- **November 14, 2022:** *Evidence-based Commentary* report deposited at D-Scholarship, the University of Pittsburgh's open access research repository.

A workflow chart (see Appendix 6) visualizes sequencing of these research stages. All students were centrally involved in course discussion of commercial surveillance. The optional assignment enabled students to self-select into research roles. Student comments in the next section (edited for formatting) were submitted both for course credit (substituting for 60% of midterm exam) and officially to the FTC in response to its ANPR call.

---

<sup>4</sup> See United States Federal Trade Commission, "FTC Extends Comment Deadline on Commercial Surveillance, Lax Data Security Practices Initiative Exploring Possible Rules," FTC Press Release, October 14, 2022, <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-extends-comment-deadline-commercial-surveillance-lax-data-security-practices-initiative>

# Comment Texts

## Comment Submitted by William Allen

The screenshot shows a public submission on Regulations.gov. At the top, it says 'Regulations.gov Your Voice in Federal Decision Making'. Below that, it indicates the document is 'Docket / Document (FTC-2022-0053-0001) / Comment'. The submission is titled 'Comment Submitted by William Allen' and was posted by the Federal Trade Commission on Nov 8, 2022. At the bottom of the submission box, there are three buttons: 'View More Comments (733)', 'View Related Comments (733)', and a 'Share' button with a dropdown arrow.

*Question 35: Should the Commission take into account other laws at the state and federal level (e.g., COPPA) that already include data security requirements. If so, how? Should the Commission take into account other governments' requirements as to data security (e.g., GDPR). If so, how?*

There is without a doubt the internet has grown to an extent it has surpassed the withholding or capabilities of the US' data privacy protection laws currently in place. Question 35 of your call for public comment asks whether the Commission should consider other governments' requirements for data security and privacy. GDPR (General Data Protection Regulation) is referenced within that question, and that is what this comment will be focused on here.

The basis of why the EU's GDPR is structurally different is because privacy and data protections are fundamental freedoms according to Title II, Article 7 of the Charter of Fundamental Rights of the European Union (E.U. 2012). Therefore, the GDPR piece of legislation controls a broader base for protection. This is clearly different than the United States' strategy of sector-based protection laws that work alongside state legislation to protect citizen's data (Kudos Data 2020). Although GDPR is in an early phase and will be continued to be monitored, a specific piece of this legislation which I think

gives it great strength aside from the hefty fines is that if you process data within the EU, you must be able to demonstrate you are GDPR compliant – I believe this regulation creates a healthy, group like atmosphere for websites that data collect as teams must keep a detailed history of what they're collecting, who's responsible for it, and may even have to appoint a data protection officer (Wolford 2022).

Creating healthy, transparent environments surrounding security and data culture can ensure organizations are set up to manage and deter malicious intrusions, threats and leaks that occur due to common human vulnerabilities. Kai Roer, author of Build a Security Culture and security awareness advocate states that companies that are successful in data competence implement and organize information surrounding data/security culture through HR (human resources) in addition to the security officer or IT roles. Companies that failed, differed in that the security officer or IT handled everything or they only focused on "checkbox compliance" (Roer 2015). The term "checkbox compliance" can reference to a lackadaisical attitude surrounding data compliance and an avoidance to dive deeper into the details of data mining. It is clear that online entities should adhere to characteristics that promote healthy data/security culture such as promoting data protection officers or roles that can take the place of an HR position surrounding the importance of data security. Implementing legislation similar to Europe's GDPR can kickstart a new wave of data security within companies in the United States.

As to specifically answer question 35, yes, the commission should consider other governments' requirements for data security and by this we explicitly mean GDPR. We should stay attentive to how the CCPA

(California Consumer Privacy Act) is playing out in one of our country's states. Regardless of impact, basic principles of the CCPA which should be implemented in all states would provide citizens the right to know what information is being collected about them, know whether their personal information is sold or disclosed and to whom, and say no to the sale of their personal information (CCPA 2022). In comparison of the CCPA vs. GDPR, disparities lie in what data is within scope; CCPA only protects data that is sold for monetary or other value considerations (releasing, disclosing, transferring, or even renting of the data), GDPR protects personal data of any type. The largest disparity lies in what organizations must adhere to respective regulations; CCPA has guidelines for only for-profit companies that collect data on California residents, have annual revenues of over \$25 million, and earn 50%+ of their revenue from California residents' data. GDPR guidelines regulate any organization that operates inside or outside the EU that offers services to EU citizens or companies. GDPR guidelines set rules for all websites that use users' data rather than CCPA's guidelines for organizations that make over \$25 million a year. The state of California should amend the CCPA to set guidelines for all data using companies rather than the large cap companies to align itself with the GDPR in that respect. Then, we should see how it is playing out in California to help ourselves decide whether to implement a nation-wide data security act like GDPR. Lastly, and a fact that carries great importance, is that Europe's GDPR bases itself of fundamental human rights outlined by the European Union while American data privacy acts do no such thing. It is surmised that

Americans will willingly support new legislation regarding online policies that adhere to their rights as human beings and through this belief and the outside research, we should adopt similar strategies.

Based on the analysis presented in this comment regarding GDPR, data/security culture, and the CCPA, the FTC should consider building a campaign surrounding the importance of a nation-wide data security act because if one is implemented soon, its impact will grow a culture of data privacy and security in years to come.

#### Works Cited

- "California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General, 28 Mar. 2022, <https://oag.ca.gov/privacy/ccpa>.
- "Charter of the Fundamental Rights of the European Union," Official Journal of the European Union 10-26-2012, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/XT>
- "EU versus US Privacy Legislation." Kudos Data, Kudos Data, 16 Nov. 2020, <https://www.kudos-data.com/blog/eu-versus-us-privacy-legislation>.
- Roer, Kai. "Chapter 7: Building Security Culture." *Build a Security Culture*, IT Governance Publishing, Ely, 2015.
- Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" GDPR.eu, 26 May 2022, <https://gdpr.eu/what-is-gdpr/?cn-reloaded=1>.

## Comment Submitted by Anonymous



The screenshot shows a public submission on Regulations.gov. At the top, it says 'Regulations.gov Your Voice in Federal Decision Making'. Below that, it indicates the document is 'Docket / Document (FTC-2022-0053-0001) / Comment'. The submission is titled 'Comment Submitted by Anonymous' and was posted by the Federal Trade Commission on Nov 8, 2022. At the bottom, there are links for 'wikipedia.org re Comments' (735), 'View Related Comments' (735), and a 'Share' button.

Techniques that manipulate consumers into prolonging online activity facilitate the commercial surveillance of children and teenagers. Many of these are especially effective on teenagers, because of the neuroscientific differences between adolescents and all other age groups. For example, techniques like social comparison and social reward- liking another person's post or getting likes on yours- is especially impactful for teenage consumers because when exposed to such stimuli, adolescents show increased activity in the ventral striatum, the reward center of the brain. Rather than gaining consumers' attention, companies discovered that getting them addicted to seeking attention from others was more lucrative (Hari 2022). These uniquely vulnerable brains call for special protections.

The Zeigarnik effect - better remembering of tasks when a person has been interrupted - is utilized by companies to keep consumers online. Bluma Zeigarnik first reported that memory is better for interrupted tasks than for completed tasks in 1927 (MacLeod 2020). If someone is pulled away from their phone or computer by a real life distraction, their first thought when this distraction is resolved will be to return to their device. These techniques facilitate commercial surveillance when applied to any age group, because more time spent online means more time for companies to collect data on what consumers do while online. This effect is magnified for teenagers, who are hyper-sensitive to social comparison, and therefore more likely to develop an addiction to this constant stream of stimulus.

50% of teens now prefer a broken bone to a broken phone (Hari 2022).

All of this makes them more susceptible to commercial surveillance and increased consumerism, which is linked to negative consequences for their mental well-being. There have been increases in adolescent depression and suicidal behaviour over the last two decades that coincide with the advent of social media (Vidal, Lhaksampa, Miller & Platt 2020). Increased sensitivity to social comparison makes social media the biggest online threat to teenagers' mental health. As seen in "The Facebook Files" (Wells, Horwitz & Seetharaman 2021), companies are well aware of the negative effects of prolonged online activity and targeted advertising on children and teenagers. Nevertheless, commercial surveillance is unavoidable. It is estimated that advertisers have at least 72 million data points on a child by the time they turn 13. The surveillance advertising industry for children is worth more than 1 billion USD. Facebook responded to concerns about the effects of surveillance advertising on children and teenagers using their apps in July 2021, claiming that they would change their practices to protect minors by removing targeted advertisements selected by advertisers, and instead using an AI delivery system to select targeted ads. While it is true that Facebook switched to an AI delivery system, the context in which this information was presented makes it 'mal-information'- genuine information shared to cause harm (Wardle & Derakshan 2017). These changes were indubitably not made in the interest of minor protection, as they have only increased the harm done to an already vulnerable population by optimizing the delivery of targeted advertisements. By turning advertising decisions over to AI systems, companies stream ever more targeted and personalized content to minors. They have proven that given a choice between protecting children and teenagers online and improving their own profits, companies will choose the

financial gain. A company's use of techniques intended to manipulate users into prolonging online activity is an unfair practice in any circumstance where the users in question are children and teenagers. The marked differences in the effects of these techniques on children and teenagers warrant special protections. Action could be taken by the FTC to create rules anchored in the statutory authority granted the FTC by virtue of COPPA.

#### Works Cited

- Abrams, Z. (2022, August 25). What neuroscience tells us about the teenage brain. American Psychological Association, <https://www.apa.org/monitor/2022/07/feature-neuroscience-teen-brain>
- Ho, E., & Farthing, R. (2021). How facebook still targets surveillance ads to teens. Fairplay, <https://fairplayforkids.org/wp-content/uploads/2021/11/fbsurveillanceport.pdf>
- Montag, C., Lachmann, B., Herrlich, M., & Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. *International Journal of Environmental Research and Public Health*, 16(14): 2612. DOI: 10.3390/ijerph16142612
- Vidal, C., Lhaksampa, T., Miller, L., & Platt, R. (2020). Social media use and depression in adolescents: a scoping review. *International Review of Psychiatry*, 32(3):235-253. DOI: 10.1080/09540261.2020.1720623
- Hari, J. (2022). *Stolen focus: Why you can't pay attention*. New York: Crown.
- Wells, G., Horwitz, J., & Seetharaman, D. (2021, September 14). Facebook knows Instagram is toxic for teen girls, company documents show. *Wall Street Journal*, [https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp\\_lead\\_pos7&mod=article\\_inline](https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp_lead_pos7&mod=article_inline)
- Macleod, C.M. (2020). Zeigarnik and von Restorff: The memory effects and the stories behind them. *Memory & Cognition*, 48(6):1073-1088. DOI:10.3758/s13421-020-01033-5.
- Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Towards an interdisciplinary framework for research and policy making*. Council of Europe Report. <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>

## Comment Submitted by Kathryn Chang

Regulations.gov  
Your Voice in Federal Decision Making

Docket / Document (FTC-2022-0053-0001) / Comment

PUBLIC SUBMISSION

**Comment Submitted by Kathryn Chang**

Posted by the Federal Trade Commission on Nov 7, 2022

View More Comments (733) View Related Comments (733) Share

*FTC Question 78: What would be the effects on consumers of a rule that required firms to give consumers the choice of being subject to commercial surveillance or withdrawing that consent? When or how often should any given company offer consumers the choice? For which practices should companies provide these options, if not all?*

Exploring the effects of a rule that required firms to give consumers the choice of being subject to commercial surveillance is a matter of redefining the dialectics of disclosure. To date, approaches to disclosure have been underwhelming. Most U.S. states do not have solidified, explicit data protection laws. This allows for mass amounts of flexibility in navigating around ambiguous and suggestive regulations that hold minimal repercussions.

One limited exception is California, which passed the California Consumer Privacy Act two years ago. The CCPA only applies to companies that generate 25 million in annual revenue and collect data for over 50,000 of California's residents. The function of the law is that people have control over where their data is being shared and to whom- accompanied by the right to sue over a data breach and the right to have their data deleted if they so choose.

Further protections must be added to this California law, as the lack of both comprehensive data protection laws and a data protection agency allows for the continuance of "abusive data practices" (EPIC, 2021). In presenting this choice to consumers, the following must be considered: the rhetoric used in the disclosure to the client, the

acknowledgment to error in judgement, and the careful examination of risks, especially ones that can taint the lives of consumers beyond the period of agreement.

While these provisions help protect consumers and also keep companies with endless resources in check, there are amendments that give consumers power that does not align in maintaining the goal of implementing accountability for bad actors in businesses. CCPA includes an amendment that closes the 30-day window for retracting data in the event of a foreshadowed lawsuit (Baig, 2022). The power shifts to consumers in that they can now sue for any security practice deemed unreasonable or not properly disclosed (i.e., the footer does not include transparency regarding what third parties are able to use their data). If consumers were given the choice to withdraw consent, then some form of a withdrawal window should be present for companies as well- CCPA can be amended to shorten the gap of data withdrawal.

Regarding the question of if consumers were given the choice of being subject to commercial surveillance- I believe that they are also given the right to waive their rights. It only becomes a matter of ethics if the consumer's data is being used to research or track an unethical activity. Consent is everything- the effect on the consumer would be kept to a minimum if they had consented to commercial surveillance. Companies, then, should offer this choice when the demographic is appropriate. The consumer must be properly informed and aware of the risks and repercussions of waiving their right to privacy.

The FTC, then, should explicitly outline what demographic that includes, as well as what practices are deemed unfair or deceptive so that consumers are well informed when their data is not protected. Consumers cannot give full consent if what they are consenting to is not clearly defined; it is in the FTC's best interest to exercise their power and resources more



productively to enforce and regulate legislation mutually serviceable for both the consumer and company.

#### Works Cited

- Baig, Anas. 2022. CCPA fines: What we know so far. *Securiti*, 13 October, <https://securiti.ai/blog/ccpa-fines/>.
- Electronic Privacy Information Center (EPIC). 2021. The FTC's unused authorities, <https://epic.org/wp-content/uploads/2021/10/EPIC-FTC-Unused-Authorities-Report-June2021.pdf>

## Comment Submitted by Colin Dyer



The screenshot shows the top of a public submission on Regulations.gov. The header includes the logo and tagline 'Your Voice in Federal Decision Making'. Below that, it indicates the document ID 'FTC-2022-0053-0001' and the type 'Comment'. The submission is titled 'Comment Submitted by Colin Dyer' and is dated 'Nov 7, 2022'. At the bottom of the submission box, there are three buttons: 'View More Comments' with a count of 733, 'View Related Comments' with a count of 733, and a 'Share' button with a dropdown arrow.

*FTC Question 15: In what circumstances, if any, is a company's failure to provide children and teenagers with privacy protections, such as not providing privacy-protective settings by default, an unfair practice, even if the site or service is not targeted to minors? For example, should services that collect information from large numbers of children be required to provide them enhanced privacy protections regardless of whether the services are directed to them? Should services that do not target children and teenagers be required to take steps to determine the age of their users and provide additional protections for minors?*

A majority of companies, websites, and social media platforms do not directly target children or teenagers. However, children and teenagers will continuously prove to be curious individuals in today's online world and find their way onto various social media platforms and websites. They have more knowledge at their fingertips than any prior generation and their access will only grow rapidly with years to come in technological advancements and the future generations of our children. Their intent to use this knowledge to their advantage will only grow as well. Ultimately, children will continuously have to evolve with technology as we already see elementary and middle schools across the country forcing children to use devices in coordination with their education.

Due to the FTC's authority stemming from Section 18 of the FTC Act, they essentially

have the right to establish what specific rules and regulations apply to various entities. While the ultimate goal of this act is to protect consumers, it also offers a robust protection for regulating businesses in general. This can work towards protecting children in that the website providers and those hosting child-oriented sites will be held liable for maintaining the protection of their users, mainly underage students. We see this argument highlighted by the FTC in their article concerning Ed Tech by Lesley Fair (Fair et al., 2022). It would be not just important but also ethically necessary to utilize these regulations to protect the young consumer. COPPA protects not only child-age internet users but also society at large from predatory companies whose sole aim is simply profit or gaining additional users.

Regardless of the age group that these sites are targeting, we should always be cautious of the fact that children will have access to them no matter what. Therefore we should always be implementing precautions to help protect our children's privacy and data. Writing about deceptive social engineering, (McNealy, 2022) states, "With few exceptions, Children's Online Privacy Protection Act (COPPA) prohibits sites directed at children under 13 years old." The million-dollar question is, how do we determine the age cut-off that these sites are directed at? Most social media platforms are not directed at children, but they still find their way onto these platforms to connect with friends or otherwise. Today, it is way too easy to lie about one's age to gain access to a social media platform, and when one is granted access, it is free range for them to browse and communicate on the site. In reality, it is nearly impossible to pin-point a certain age demographic that are accessing platforms and websites. So, we must always keep the expectation that minors will be accessing the sites in order to deter any harm that could come to these children from the collection of their data.

For example, take the new social media app “BeReal” that was launched in 2020 and gained a widespread popularity with over 10 million daily users in August of 2022 (Sklenkar, 2022). The app is open to users over the age of 13 and involves a daily post at a random time that can be seen by your friends, or anyone in the world depending on your privacy settings. If one’s account is public, it records your exact location and displays it on a map to anyone else on the app. Now, considering that the app is not directly targeting children, the ones that do have the app are at a significant risk when it comes to their personal information. Imagine a 13-year-old girl posts publicly on the app from her home. Anyone that sees her post now has the exact location of her house and knows what she looks like. It’s also safe to assume children as young as 11 and 12 have downloaded the app to participate with their older friends who are above the 13-year-old age limit. Moreover, from a more personal point of view, if my friends and I had lied about our ages to make a Facebook account in 2012, what is stopping these minors from doing the same thing with present day social media platforms?

Whether it comes down to children using technology for education, entertainment, or just pure curiosity, they should never have to worry about either inadvertently creating a digital footprint, or their personal information

being stored or unduly distributed. To directly answer the FTC’s question, services that do not directly target children should, in fact, be required to take steps to determine the age of their users, further protecting the privacy of minors in this country.

#### Works Cited

- McNealy, J. E. (2022). Platforms as phish farms: Deceptive social engineering at scale. *New Media & Society*, 24(7), 1677–1694.  
<https://doi.org/10.1177/14614448221099228>
- Fair, L., et al. (2022, August 11). FTC to Ed Tech: Protecting kids' privacy is your responsibility. Federal Trade Commission. Retrieved October 18, 2022, from <https://www.ftc.gov/business-guidance/blog/2022/05/ftc-ed-tech-protecting-kids-privacy-your-responsibility>
- Sklenkar, A. (2022, October 12). 18 stats to know about bereal app (updated Oct. 7th, 2022). Online Optimism. Retrieved October 17, 2022, from <https://www.onlineoptimism.com/blog/bereal-stats-app-figures-data-be-real-numbers-toknow/#:~:text=BeReal's%20app%20currently%2C%20in%20August,in%20the%20last%20year9>

## Comment Submitted by Austin Hogeboom

Regulations.gov  
Your Voice in Federal Decision Making

Docket / Document (FTC-2022-0053-0001) / Comment

**PUBLIC SUBMISSION**

**Comment Submitted by Austin Hogeboom**

Posted by the **Federal Trade Commission** on Nov 8, 2022

[View More Comments](#) 733 [View Related Comments](#) 733 [Share](#)

*FTC Question 19: Given the lack of clarity about the workings of commercial surveillance behind the screen or display, is parental consent an efficacious way of ensuring child online privacy? Which other protections or mechanisms, if any, should the Commission consider?*

*FTC Question 20: How extensive is the business-to-business market for children and teens' data? In this vein, should new trade regulation rules set out clear limits on transferring, sharing, or monetizing children's and teens' personal information?*

The presence of technology in the lives of children is ever-increasing, and so is its degree of necessity for educational purposes, especially in the wake of the COVID-19 pandemic. The urgent need for continued education during the pandemic meant that suddenly, most American school-aged children had been transferred to online-based learning. School districts were forced to not only navigate the pandemic and the policies required of them but also to negotiate contracts with technology companies, with a shark-like interest in expanding their business into the education market. The details of some of these contracts are murky, and despite being publicly available (via Freedom of Information Act requests), are not easily understood. Major tech companies hold an increasingly large presence in the average American classroom through educational technology suites like G-

Suite for education from Google. These companies harvest data from students and teachers to optimize the educational experience, but the potential for anecdotal data to inform decisions for non-educational technology products still exists despite COPPA. This leaves parents and children as young as kindergarten in a disadvantaged situation, as their data security and internet privacy are left to the hands of school boards and business executives.

Student technology initiatives such as 1-1 programs, which place a device in the hands of a student for the entire school year (in and out of class) have become a lot more popular since the onset of the pandemic. These programs allow students the ability to access schoolwork 24/7 and many teachers have used this expanded capability to great educational advantage, requiring work to be done exclusively online. But when the fact that most schoolwork is required to be completed online, with school-issued devices being utilized in the home, parents are almost forced to accept these vague digital use contracts or risk disadvantaging their child's education.

These parents are forced to place more trust in school boards and superintendents to negotiate contracts in the best interests of their children and family preferences. Educational technology providers, such as Google, who just recently acquired a data analytics firm specializing in the educational market, cannot be necessarily guaranteed to have the best interest of students in mind. Having such educational devices set up in the home exposes not just the student to the potential harms of unchecked or unwanted surveillance, but also the parents, siblings, and home wifi network as well. Providing hardware and software in the name of bringing students and educators fully into the post-pandemic 21st century must not absolve school officials' responsibility to

ensure the safety and security of students' data.

I understand the FTC has made a strong commitment to enforcing COPPA in EdTech, but the processes of this strategy are only on a retroactive, case-by-case review system. The FTC should take an active, hard look at how the business-to-business market in the educational sphere creates risks for children's data inside and outside the classroom in the post pandemic landscape. The data protection of school-age children deserves consideration for the legislation of new rules and restrictions by the Commission. This is supremely necessary especially in areas where students, nor the parent or guardian can explicitly consent to the terms by which their child's educational success depends on.

#### Works Cited

- Federal Trade Commission. (2022, May 19). Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act. Washington, D.C.; Federal Trade Commission. Retrieved October 20, 2022, from <https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection>
- Mollenkamp, D. (2022, October 11). Google discreetly acquires Edtech analytics company BrightBytes. EdSurge. Retrieved October 20, 2022, from <https://www.edsurge.com/news/2022-10-11-google-discreetly-acquires-edtech-analytics-company-brightbytes>
- Natanson, H. (2020, April 19). Failed tech, missed warnings: How fairfax schools' online learning debut went sideways. *The Washington Post*. Retrieved October 20, 2022, from [https://www.washingtonpost.com/local/education/fairfax-schools-online-learning-blackboard/2020/04/18/3db6b19c-80b5-11ea-9040-68981f488eed\\_story.html](https://www.washingtonpost.com/local/education/fairfax-schools-online-learning-blackboard/2020/04/18/3db6b19c-80b5-11ea-9040-68981f488eed_story.html)

## Comment Submitted by Lukas Kim



The screenshot shows the Regulations.gov website interface. At the top, it says "Regulations.gov Your Voice in Federal Decision Making". Below that, it indicates the document is "Docket / Document (FTC-2022-0053-0001) / Comment". The main heading is "PUBLIC SUBMISSION" followed by "Comment Submitted by Lukas Kim". It notes the comment was "Posted by the Federal Trade Commission on Nov 7, 2022". At the bottom of the comment box, there are buttons for "View More Comments" (733), "View Related Comments" (733), and a "Share" button.

*FTC Question 1: Which practices do companies use to surveil consumers?*

Companies have multiple ways of surveilling their consumers, some of which are less obvious than others. One of these methods is that the companies scan their users' personal data, their browsing history, interactions on posts, viewing time on content, etc., and collect it to build a profile that is then used to deliver advertisements that are catered to whatever the person's interests are. Johann Hari states that these profiles are like "voodoo dolls". They start out basic and average, but as you keep on going through websites, clicking on posts, and reading articles, that voodoo doll collects this information like different parts of you, adding it to itself in order to understand what would keep your interest the most (Hari) Apps like Facebook are monetized by how long you're on the site, every second is another cent. So, it's obvious that they would want to keep you on as long as possible with these targeted ads and filtered content that sends you on a downward spiral to page after page of content until you lose seconds, minutes, hours of your life mindlessly scrolling and reading while they profit off of it. There are also "cookies" and "web beacons" that enable companies to track browsing histories. The way that cookies work is that they're small files, unique identifiers like a fingerprint that web servers send to browsers. These cookies can then be sent back to the server every time your browser opens a new tab, giving that website a way to

remember you, your preferences, and online habits (HP Tech Takes). Web beacons work in a similar way except they can be delivered through a web browser or an email. Companies can also act as data aggregators, purchasing or sourcing consumer data from third parties to then sell to other third parties. It's not just your laptops or computers that can be tracked either. Mobile phones have their own ways to track your activity like third-party SDK's (Software Development Kit's), which are normally used as software building tools, that can source consumer data as well.

In light of the various techniques of surveillance detailed in this comment, the FTC should create some sort of regulation or strategy to decrease the amount of information that websites are allowed or able to take from users on their site. Whether it is a specific amount of information or only a certain type of information that they are allowed to collect. The specifics on those criteria can be determined by the FTC at their own discretion.

### Works Cited

- Johann Hari, "Cause Six: The Rise of Technology That Can Track and Manipulate You (Part Two)" (Chapter 7) in *Stolen Focus* (New York: Crown, 2022): 124-155
- How do companies collect data? Narrative Knowledge Base. (n.d.). Retrieved October 6, 2022, from <https://kb.narrative.io/how-do-companies-collect-data>
- Computer cookies: What they are and how they work (infographic). Computer Cookies: What They Are and How They Work (Infographic). (n.d.). Retrieved October 6, 2022, from <https://www.hp.com/us-en/shop/tech-takes/what-are-computer-cookies#:~:text=How%20Do%20Cookies%20Work%3F,preferences%2C%20and%20your%20habits%20online>.
- SDK vs. API: What's the difference? IBM. (n.d.). Retrieved October 6, 2022, from <https://www.ibm.com/cloud/blog/sdk-vs-api>

## Comment Submitted by Kamryn Kostelnik



The screenshot shows the Regulations.gov interface. At the top, it says "Regulations.gov Your Voice in Federal Decision Making". Below that, it indicates the document is "Docket / Document (FTC-2022-0053-0001) / Comment". The main heading is "PUBLIC SUBMISSION" followed by "Comment Submitted by Kamryn Kostelnik". It notes the comment was "Posted by the Federal Trade Commission on Nov 7, 2022". At the bottom, there are three buttons: "View More Comments 733", "View Related Comments 733", and "Share".

*Question #67: How should the Commission address such algorithmic discrimination?*

The prevalence of algorithmic discrimination based on protected categories such as race, sex, and age is escalating. Through data collection, platforms can create algorithms that determine which advertisements and particular online content will appeal to the user. Furthermore, many advertisers and regulators fail to fully assess how these algorithms facilitate discrimination. Algorithmic discrimination marginalizes users through a lack of exposure to loan, employment, and housing content, expanding upon already existing racial disparities.

In addition, users of these platforms can also be victims of voter suppression, voter deception, and diluting the voting power of communities of minorities. In an article published by The New York Times, Shane Scott and Sheera Frenkel explain how the Russian Internet Research Agency targeted African American voters on social media platforms. Scott and Frenkel state, "The most prolific I.R.A. efforts on Facebook and Instagram specifically targeted black American communities and appear to have been focused on developing black audiences and recruiting black Americans as assets. Using Gmail accounts with American-sounding names, the Russians recruited and sometimes paid unwitting American activists of all races to stage rallies and spread content, but there was a disproportionate pursuit of African Americans" (Scott and Frenkel).

The FTC's current method of addressing algorithmic discrimination may not be most effective. During the September 8th public forum, Spencer Overton, President of the Joint Center for Political and Economic Studies, discusses why a "case by case" approach to regulating commercial surveillance is not always effective. Overton argues that "litigation on a case-by-case basis is an important tool but it's not always the best way to prevent or deter discrimination before it occurs."

The whole basis of the case-by-case approach essentially ensures that acts of discrimination must occur and be brought into question before being assessed and dealt with by the FTC. Furthermore, the case-by-case approach facilitates further discrimination by not providing one set of standards for identifying and dealing with the issue. This allows the individual in charge of the case to deal with it as they see fit.

A rulemaking approach may be a more effective way to prevent discrimination before it occurs. Having a known set of standards and regulations sets the precedent to companies that acts of discrimination will be penalized. I believe this approach adds a greater sense of accountability to companies who break the rules. Additionally, knowing the consequences for their actions would aid in deterring these companies from using algorithmic discrimination in the first place. The FTC should consider trying a rulemaking approach for dealing with discrimination to ensure platforms do not have the right to maximize their profits through discriminatory advertisement distribution onto both economically and politically marginalized groups.

## Works Cited

Overton, Spencer. 2022. Statement. Commercial Surveillance and Data Security Public Forum. September 8. U.S. Federal Trade Commission, [https://www.ftc.gov/system/files/ftc\\_gov/pdf/CommercialSurveillanceandDataSecurityRulemakingTranscript09.08.2022.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/CommercialSurveillanceandDataSecurityRulemakingTranscript09.08.2022.pdf).

Shane, Scott, and Sheera Frenkel. "Russian 2016 Influence Operation Targeted African-Americans on Social Media." The New York Times, The New York Times, 17 Dec. 2018, <https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html>



## Comment Submitted by Alyssa Morales



The screenshot shows the Regulations.gov website interface. At the top, it says "Regulations.gov Your Voice in Federal Decision Making". Below that, it indicates the document is "Docket / Document (FTC-2022-0053-0001) / Comment". The main heading is "PUBLIC SUBMISSION" followed by "Comment Submitted by Alyssa Morales". It notes the comment was "Posted by the Federal Trade Commission on Nov 7, 2022". At the bottom of the comment box, there are three buttons: "View More Comments" with a count of 733, "View Related Comments" with a count of 733, and a "Share" button with a dropdown arrow.

*FTC Question 4: How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?*

During the FTC Commercial Surveillance and Data Security Public Forum on September 8, 2022, Karen Kornbluh discussed the criminalization of user data collection on websites and social media platforms. Kornbluh is the leader of the U.S German Marshall Fund’s digital innovation and democracy initiative. The initiative works to ensure “that technology supports rather than undermines democracy” and protects the rights of consumers as citizens (Kornbluh). Kornbluh asserts that sites unethically collect sensitive user information and use it to target certain groups of people. Kornbluh referenced one company who was “revealed to sell data identifying people visiting planned parenthood clinics,” using heat maps “to trace clinic visitors to specific homes” (Kornbluh). As referenced by Kornbluh, heat maps can be used to trace consumers’ locations, store the location data in a cache, and sell the data to other entities, such as advertisers. Advertisers can use the location data to tailor their advertisements to consumers based on where they live. This data can be used to discriminate against people. Many clinics, for example, are located in lower-income and predominately minority neighborhoods. Advertisers can use this data to target low-income people and minority groups. Most people who attend Planned Parenthood clinics are women, and advertisers could use this data to discriminate against women.

There have been numerous examples of advertisers using user data collection to discriminate against people. In 2019, Facebook was revealed to “discriminate against marginalized groups including women, people of color, and the elderly” (McNealy). Facebook advertisers were targeting users by age, gender, and geographical location by showing them specific advertisements for housing, employment, and credit offers. Facebook advertisers were also excluding certain groups from these advertisements altogether. For example, if user data indicated that someone lives in a low-income, predominately minority neighborhood, they would be excluded from seeing high-paying job offers. The company settled five discrimination lawsuits and agreed to change their policies on targeted advertisements (Gillum and Tobin). Tracking people who have visited Planned Parenthood clinics can have similar consequences, as many people visiting these clinics are part of these marginalized groups, such as women, low-income people, and people of color.

Following the *Dobbs vs. Jackson Women’s Health* (2022) decision to overturn the federal right to abortion, companies can also use sensitive information to target voters (Supreme Court of the United States). Collecting location data of users who visit Planned Parenthood clinics allows companies to manipulate the type of political content users see. This could lead to people being manipulated to vote for or against an issue or politician without having full knowledge of such issues or politicians. Collection of sensitive user data removes the freedom for users to make their own decisions on what content they consume. It forces users to consume select pieces of information and content targeted to them by a large company. It is manipulative and prevents people from doing their own research and making their own decisions based on that.

I agree with Kornbluh and argue that the collection of sensitive user data and “the criminalization of our private lives” is unethical (Kornbluh). It removes people’s right to make their own decisions on what jobs or houses they apply for, who they vote for, and so on. It is not enough to evaluate data collection practices on a case-by-case basis anymore. Case-by-case evaluations fail to hold all companies accountable and ensure ethical data collection practices. The FTC must enact broad rules that prohibit companies from collecting sensitive user data and using it to target consumers through advertisements and tailored content. There should also be constraints as to what kind of user data can be collected. Location data collection is particularly harmful to people as it invades people’s privacy and can be used to discriminate against people based on where they live and where they go. People’s location of residence and daily outings, such as visiting a Planned Parenthood clinic, are private and should not be used to manipulate content. The collection of user data for political purposes is also extremely unethical and a threat to democracy. It manipulates voters to support or oppose political viewpoints without having sufficient knowledge on the viewpoints. There should also be more transparent consent policies. Companies should communicate

clearly to users their data collection practices and give users the choice to make an informed decision to consent or not.

#### Works Cited

- Gillum, Jack, and Ariana Tobin. “Facebook Won’t Let Employers, Landlords or Lenders Discriminate in Ads Anymore.” ProPublica, 19 Mar. 2019, [www.propublica.org/article/facebook-ads-discrimination-settlement-housing-employment-credit?token=tCCj21-FHUtoVSuy7QOrlXw0rpazS0Qn](http://www.propublica.org/article/facebook-ads-discrimination-settlement-housing-employment-credit?token=tCCj21-FHUtoVSuy7QOrlXw0rpazS0Qn).
- Kornbluh, Karen. Commercial Surveillance and Data Security Public Forum, Federal Trade Commission, 8 September 2022. Panelist.
- McNealy, Jasmine E. “Platforms as Phish Farms: Deceptive Social Engineering at Scale.” *New Media and Society*, vol. 24, no. 7, July 2022, [doi.org/10.1177/14614448221099228](https://doi.org/10.1177/14614448221099228).
- Supreme Court of the United States. *Dobbs v. Jackson Women’s Health Organization*. Docket no. 19-1392, 24 June 2022. Supreme Court of the United States, [https://www.supremecourt.gov/opinions/21pdf/19-1392\\_6j37.pdf](https://www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf). PDF download

## Comment Submitted by Marlo Postufka



The screenshot shows a public submission on the Regulations.gov website. At the top, it says "Regulations.gov Your Voice in Federal Decision Making". Below that, it indicates the document is "Docket / Document (FTC-2022-0053-0001) / Comment". The submission is titled "Comment Submitted by Marlo Postufka" and was posted by the Federal Trade Commission on Nov 7, 2022. There are buttons for "View More Comments" (733), "View Related Comments" (733), and a "Share" button.

*FTC Question A4: How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?*

*FTC Question A5: Are there some harms that consumers may not easily discern or identify? Which are they?*

In response to question A4, each social media organization ultimately prioritizes their growth, driven by specialized advertisements and personalization absent consumer consulting. Thus, I think it is crucial that the FTC develop rules to ensure the protection of consumers, especially considering large-scale social media. With increasing social media, coupled with big data, users are having advertisements that are more catered toward them, which ultimately hinders their ability to not only explore other opinions, but negates the concept of free will. Free will, here thought of as autonomy to communicate and act in accordance with individual beliefs and wants, is compromised by social media platforms, as these platforms utilize targeted ads to prevent consumers from making choices freely.

Sites prioritize growth of their company through exploiting consumers to yield revenue and claiming "growth" is a way to hide behind the deceptiveness of it all. Additionally, the algorithmic editing of the internet mitigates the freedom of media. It moves consumers to see and engage with items that the algorithm thinks they need to view, rather than what they need to see. According to McNealy, "...social

platforms like Facebook, Twitter, and [other social platforms] are large-scale phishing operations designed to collect information about users deceptively and surreptitiously" ("Platforms as phish farms"). Consumers ultimately have no choice about who serves as social media gatekeepers, as this is left to algorithms that know much more about them than consumers know about the algorithms. Thus, this poses a direct harm and risk to consumers.

In response to A5, the concept of dark patterns blatantly weaponizes free will. According to Arvind Narayanan and colleagues, "dark patterns are user interfaces that benefit an online service by leading users into making decisions they might not otherwise make" ("Dark Patterns Past, Present, and Future"). Free will can be thought of as freedom from unwarranted deception and manipulation in choice making. Natasha Dow Schull, details in her book *Addiction by Design* how gambling negates free will. Although it may appear that a compulsive gambler is exercising free will every time they pull a slot or return to the casino, however, casinos are designed to hook compulsive gamblers through persuasive techniques. Thus, free will is being compromised, especially in addictive settings, as consumers are "made" to be addicted to such marketing techniques, like specialized or interactive ads. This ultimately evades humans' autonomy to make choices based on exploiting users and their cognitive biases. By having the retailers and or companies determining a user's fate without their knowledge or consent that their information would be manipulated/abused is completely inequitable. Dark patterns ultimately strive to change the behavior of a user (who presumably lacks knowledge in said market) to benefit the company or "retailer." While it technically works, it is blatantly deceptive and manipulative, which negates the concept of transparency -- a true concern of the FTC, as "federal privacy legislation would provide transparency to consumers regarding the full

scope of data collection, and how collected data are used, shared, sold, and otherwise monetized" (US FTC, "Trade Regulation Rule"). Additionally, user agreements are often wordy and opaque in the sense that superfluous information is put for the sole purpose of discouraging a user from reading the agreement in its entirety. Thus, it can be argued that this is a dark pattern in and of itself. In an effort to combat this, perhaps the FTC can implement rules, such as having a word count limit, or page limit, or utilizing bold letters for crucial information. With social media today, the question as to how much freedom each consumer truly has in the realm of the online world is pertinent and must be asked. Ultimately, the normalization of dark pattern advertising makes case-by-case unworkable, given the scale of deception.

In conclusion, the FTC needs to address the way in which data is utilized from a "retailer" perspective, as well as phishing, and dark patterns. These concepts are ultimately hindering the free will of humans, as well as presenting an ultimate danger to these individuals by blatantly taking advantage of consumers and their personal data; it could even be argued that certain rules, such as section 18, which focuses on combating harms posed to consumers, needs to be revised,

because these risks are not being consistently addressed.

#### Works Cited

- Lee, Kah-Wee. (2014). Addiction by Design: Machine Gambling in Las Vegas by Natasha Dow Schüll (review). *Technology and Culture*. 55. 278-280. doi:10.1353/tech.2014.0015.
- McNealy, Jasmine. (2022). Platforms as phish farms: Deceptive social engineering at scale. *New Media & Society* 24, 1677-1694 doi:10.1177/14614448221099228.
- Narayanan Arvind, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. (2020). Dark patterns: Past, present, and future. *Queue* 18(2), <https://dl.acm.org/doi/10.1145/3400899.3400901>.
- United States. Federal Trade Commission. (2022). Trade regulation rule on commercial surveillance and data security. Advance notice of proposed rulemaking. August 8, <https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security>.

# Appendices

## Appendix 1: FTC Public Forum Scouting Assignment

The Federal Trade Commission is holding a [public forum](#) on "Commercial Surveillance and Data Security," Thursday, Sept 8, 2022, 2:00 - 7:30 p.m. (access webcast [here](#) and written transcript [here](#)). Note: As of Sunday morning, the link used for the live feed can now also be used to view the public forum recording retrospectively.

To prepare for our discussion of the assigned Palczewski, Ice, and Fritch reading for Tuesday, Sept 13, please complete the following "FTC Public Forum Scouting" assignment:

- **Watch** at least one 5-minute segment of the FTC public forum (you can tune in live at any time between 2:00-7:30 p.m.) You may want to consult the agenda to pop in during a speaker or session you find particularly interesting. Feel free to watch more than one 5-minute segment, but in the end pick one select one segment to report out to a small group on Tuesday, Sept 13.
- Come to class Sept 13 prepared to **describe**, *in one concise sentence*, what you saw and heard during the 5-minute segment you selected to engage. Think about adding specifics such as: a) speaker; b) topics covered; c) evidence presented.
- Come to class Sept 13 prepared to **explain**, *in one concise sentence that incorporates one of the "key themes" from Palczewski, Ice and Fritch (isolated on the syllabus)*, what was your **key takeaway** from the 5-minute segment you selected to engage?

Hint: We will be using Google Jamboard on Sept 13, so please come to class with an internet-capable device and think about ways you might express what you describe and explain visually (e.g. with visual image or representation).

## Appendix 2: FTC Public Forum Jamboard Assignment

**FTC Public Forum Jam (September 13):** Link to Google Jamboard is [here](#). This [quick Jamboard tutorial](#) may help you get oriented if you do not find the interface intuitive. Procedure:

- **Find** your group. If you completed the Discussion Board assignment above by Sept 12, you will have already been sorted into a group that corresponds to the topic area identified in your scouting (just locate your name in the sticky note below a group). If you did not post on the Discussion Board, you can catch up during class by picking a group based on your interests. Once you have identified a group to join, move to one of the six locations on the room map that corresponds to your group number, and add your name, if needed, to the sticky note below the group number on the Jam map.
- Add content to your group's Jamboard: **1) Describe**, in one concise sentence, what you saw and heard during the 5-minute segment you selected to engage. Think about adding specifics such as: a) speaker; b) topics covered; c) evidence presented; **2) Explain**, in one concise sentence that incorporates one of the "key themes" from *Palczewski, Ice and Fritch* (isolated on the syllabus), what was your **key takeaway** from the 5-minute segment you selected to engage. "Sign" your contribution by adding your first name at the end of your contributed content like this: (Gordon).
- **Discuss**, with your other group members, what you see emerging from your Jamboard after each person has added content. Are there common themes emerging? Note the FTC's hand-picked question prompts to the left: Are there ways that the content begins to suggest answers to the question prompts? Does the content suggest avenues for future research? Feel free to add images and URLs to express your ideas, and consider moving content around to illustrate connections or proximity of content. If appropriate, continue adding written content to the Jamboard to reflect the outcome of these discussions, and/or prepare to share it verbally, by nominating one student to report during wrap-up group share-outs near the end of class. If you feel like your Jamboard is getting overstuffed with content, consider creating one spillover/companion Jamboard to accompany your initial creation.

## Appendix 3: Jamboard Assignment Work Product Example

### Group 6 Discrimination

d(65) How prevalent is algorithmic discrimination based on protected categories such as race, sex, and age?

d(66) How should the Commission evaluate or measure algorithmic discrimination?

d(67) How should the Commission address such algorithmic discrimination?

d(58) Could new rules help ensure that firms' automated decision-making practices better protect non-English speaking communities from fraud and abusive data practices? If so, how?

(a)12. How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors?

Spencer Overton, President of Joint Center for Political and Economic Studies, discusses how data collection & developed algorithms on social platforms facilitate discrimination.

He further supports his claim by providing various examples, specifically the Meta vs. DOJ court case.

The speaker made a claim of fact: Housing ads are being targeted towards certain users and discriminating against others, and suggested a probable outcome: that allowing this to continue could automate racial

Platforms like Facebook and Google used user information to target ads in ways that could sometimes be discriminatory- for example, ads for new housing being steered towards White users and away from Black and Latinx users.

Harlan Yu (Executive Director of Upturn): Commercial data collection exacerbates racial and class-based discrimination, furthering existing economic biases and outcomes

The personal sphere has become completely obfuscated by the technical sphere; livelihood, meaningful community, and progress are policed by those with

money/advantage at the cost of continued denigration of marginalized groups

What is the public good served by collecting economic data? Is unhousing people a way to build community, strengthen the economy, promote economic equity?

Does this widespread discrimination truly count as "case-by-case" when it is inflicted en masse upon protected classes of people?

"Also litigation on a case by case basis is an important tool, but it's not always the best way to prevent and deter discrimination before it occurs"

There is an increasing support for the claim that the technical sphere of argument alone may not be the best way to prevent discrimination.

KJ Bakji, Senior Director of Technology Policy at The Chamber of Progress- Supporting the FTC's policy notion to protect consumers from being discriminated upon based off of personal data

The Commission could best evaluate or measure algorithmic discrimination by creating a baseline guide of rule(s) and/or regulations as a measuring stick to not only regulate and put restraints on companies as

"And although some of these practices are new due to the proliferation of digital data and predictive technologies across society, discriminatory outcomes are historical, they are longstanding and they remain essential

story in today's economy and in people's everyday lives."

When discrimination is addressed case-by-case, it leaves massive gaps of time and opportunity during deliberation. That time is filled by a class of individuals being economically disadvantaged, unhousing, and out of work.

Regulation rules need to look at "unintended" harms caused by companies' intended effects. There cannot be room for "accidental" discrimination.

I would argue this discrimination, because it is historical, IS in fact intended and is weaponized against marginalized groups by those who pay for data and control livelihood

Arguments for data collection/utilization tend towards definitional; they are defining a "good" person or neighbor or employee with narrow, historically racist and classist terms.

## Appendix 4: Adjacent Curriculum Description

### Midterm pre-write (FTC public comment)

Published

Edit



This is a purely optional assignment. Students wishing to take the full regular midterm exam can pass on this option, with no grade penalty. However, students opting in to write a FTC public comment can earn up to 30 points (60% of the midterm exam points - substituting for three, 10-point short answer questions) by:

- Submitting a draft of their FTC public comment to a Canvas Discussion Board by October 6, 2022, 11:59 p.m. This will facilitate peer review.
- Submitting a revised, final version of their FTC public comment here by **October 18, 2022, 11:59 p.m.** Your final comment will then be graded, and it will be purely up to you whether you choose to submit the comment to the FTC (note their Oct 21 deadline).

Comment guidelines:




- Prompt: Choose one or more questions from the FTC's ["List of 95"](#) in their call for public comment on commercial surveillance rulemaking and contribute an evidence-based response.
- Minimum 300 words, no maximum.
- Provide citations for all source references, consistently applying a citation style of your own choosing. Visit Pitt [Library's guide](#) to make a choice and find instructions for how to apply the style to your document.

#### Frequently Asked Questions

- *If I opt-in to this assignment, how will my grade be included into my midterm?* Simply write "see FTC public comment assignment" in the midterm's short answer text box (no need to write full answers), and your grade from this optional assignment will be folded into your midterm exam grade.
- *If I opt-in to this assignment, can I also write the short answer section of the midterm?* Yes - your best score (out of 30 points) will be used.
- *Do I have to cite course materials for theoretical concepts?* Yes. Consult the syllabus for citations.
- *Where do I submit my paper?* Two places: 1) A preliminary rough draft to a Discussion Board by October 6, 11:59 p.m.; 2) Here, in an assignment text box, by October 18, 11:59 p.m.
- *Do I have to actually submit my final comment to FTC in order to earn credit?* No. Your comment will be graded using the assignment rubric, independently of whether you ultimately decide to submit it to the FTC.
- *When does the FTC public comment window close?* October 21, 2022, so you have a full week between the due date for submitting your public comment for grading here and the deadline for FTC public comment submissions.



## Appendix 5: Optional Assignment Grading Rubric

<b>FTC Public Comment</b>			
  			
You've already rated students with this rubric. Any major changes could affect their assessment results.			
Criteria	Ratings		Pts
<b>Timeliness</b> A draft comment was submitted to a Discussion Board by Oct 6, 2022, 11:59 p.m.. and a revised final comment was submitted here by Oct 13, 2022, 11:59 p.m.	<b>5 pts Full Marks</b>	<b>0 pts No Marks</b>	5 pts
<b>Prose quality and citation practice</b> The comment features strong and polished prose, free from significant typographical and/or grammatical errors, relevant references are cited, consistent with a selected style guide.	<b>10 pts Full Marks</b>	<b>0 pts No Marks</b>	10 pts
<b>Prompt responsiveness</b> The final comment responds cogently to one or more of the FTC's "List of 95" questions in its call for public comment on commercial surveillance rulemaking (be sure to identify specific questions your comment addresses to maximize opportunity for full credit in this criterion - this can be done easily by simply cutting and pasting the text of the question(s) and beginning your comment with them).	<b>10 pts Full Marks</b>	<b>0 pts No Marks</b>	10 pts
<b>Evidence-based approach</b> The comment shows an evidence-based approach by drawing from, and citing properly, at least one concept from the Evidence course reading list, as well as incorporating and citing other evidence to support your position.	<b>5 pts Full Marks</b>	<b>0 pts No Marks</b>	5 pts
			Total Points: 30

### Appendix 6: Optional Assignment Workflow Chart

