ADL
FIGHTING HATE FOR GOOD™

Honorable Commissioners
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580

Re: Commercial Surveillance ANPR, R111004

Dear Commissioners,

ADL (the Anti-Defamation League) submits these comments urging the Federal Trade Commission (FTC) to implement a new trade regulation rule that adequately addresses the significant impact of surveillance advertising and data security practices on the spread and impact of hate and extremism. The comments below are submitted in support of R111004 to address these issues and, specifically, the ways in which surveillance advertising deployed by tech companies causes harm by fueling hate and misinformation.

ADL is a leading anti-hate organization founded in 1913 to stop the defamation of the Jewish people and to secure justice and fair treatment to all. ADL has unique expertise in fighting hate online because of the organization's work at the intersection of civil rights, extremism, and technology, and because we are rooted in and draw upon the lived experience of a community that has been relentlessly targeted online by extremists and bigots. In 2017, ADL launched the Center for Technology and Society (CTS), a research-driven advocacy center that works to end the proliferation of online hate and harassment. CTS partners with industry, civil society, government, and targeted communities to expose these harms, hold tech companies accountable, and fight for just, equitable online spaces. Further, ADL has introduced national initiatives such as PROTECT, COMBAT, and REPAIR, which focus on advocating for policies to counter the surge of violent domestic extremism, antisemitism, and online hate.

The comments below address the societal harm surveillance advertising creates as a toxic incentive system where Big Tech perpetuates, amplifies, and normalizes hate and extremism.

Over the past several years, ADL has called out the fact that surveillance advertising–the fundamental business model that large tech companies rely on–is a key driver of the hate and violence we see normalized online and moved offline. Under Section 18 of the FTC Act, 15 U.S.C. Sec. 57a, the Commission is authorized to prescribe "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce" within the meaning of Section 5(a)(1) of the Act and these rules are known as "trade regulation rules."[1] Thus, we respectfully request that the FTC, under its rule making authority, consider the grave harm caused by surveillance advertising and lax data practices and provide meaningful consideration to the comments submitted in support of new trade regulation rule, R111004.

Surveillance advertising incentivizes platforms to favor hate and extremism

Tech companies' fundamental business model—surveillance advertising—maximizes profits because the astronomical amount of data collected on every user enables platforms to target them with the content and recommendations best designed to keep those users engaged on the platform for as long as possible in order to serve them with as many ads as possible. To do that, social media companies constantly track users' online behavior (on and off an individual platform), collect their data, and feed it to algorithms that are optimized to recommend engaging content that will make them click, like, comment on, and share. The longer users spend online and the more engaged they are, the more data social media companies can collect to predict what content will engage those users even more. Then, social media companies serve that content to those users, and sweep up even more data in order to recommend more and better-targeted ads to those same users. This is a self-perpetuating loop.

Increasing engagement on social media platforms for the purpose of making more and more ad revenue, no matter the societal cost, is the overarching goal toward which platform function is designed. It remains the most important metric of success for these companies. Whether the platforms intentionally designed their algorithms to inflame hateful content is not the point. Once the goal of maximizing engagement above all else is decided upon and coded into the algorithm, and is not materially changed or stopped, then the consequences described here are inevitable. Without interventions from a number of sources, including adoption of the rule at issue here, these consequences will only get worse.

Certainly a growing body of research—including research conducted by ADL—demonstrates that controversial, hateful, and polarizing information and misinformation are often more engaging than other types of content and, therefore, receive wider circulation.[2] That is why platforms' algorithmic tools significantly boost extremist content, from white supremacist groups and Holocaust denial to COVID-19 hoaxes and other forms of misinformation.[3] Platforms privilege and promote this content to create a stimulus–response loop. In fact, reports of a Facebook researcher who explored how the social media platforms deepened political divides

[1] *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*. (2021, May). Federal Trade Commission. https://www.ftc.gov/about-ftc/mission/enforcement-authority

[2] *Facebook's Hate Speech Problem Is Even Bigger Than We Thought*. (2020, December 23). ADL. https://www.adl.org/blog/facebooks-hate-speech-problem-is-even-bigger-than-we-thought

[3] Greenblatt, Jonathan. *Congressional Testimony: Holding Big Tech Accountable: Legislation to Build a Safer Internet*. (2021, December 09). House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce. https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Greenblatt_CPC_2021.12.09_1.pdf

illustrated the speed with which platform algorithms get to work to recommend content rife with misinformation and extremism: less than a week.[4]

The tech companies have known this for years. For example, more than three years ago, in 2019, an internal Facebook report on hate and misinformation had found "compelling evidence that our core product mechanics, such as virality, recommendations, and optimizing for engagement, are a significant part of why these types of speech flourish on the platform" and concluded that the company was actively promoting these types of activities.[5] Other platforms similarly both engaged in their own research and were provided with external research showing how much more engaging hate and extremist conspiracy content is when compared to other types of content, how quickly their recommendation functions led users to the most extreme content and introduced them similarly enticed to that content, and how frequently mass shooters and other violent perpetrators had engaged with this content in the lead up to their acts. The platforms' reaction was nearly always one of denial and counter-attack, or at most, of tinkering on the edges for a while until public or legislative attention moved on.[6]

The continuous amplification of hate, bigotry, and conspiracy theories—which is core to social media platforms' surveillance advertising business model—has created an environment for extremism to flourish. As highlighted by ADL in Congressional Testimony, "QAnon and its consistent elevation of antisemitism, the mainstreaming of the foundational white supremacist "Replacement Theory," #StoptheSteal, and COVID conspiracies all are examples of extremism and hate that have become increasingly normalized and mainstreamed—in large part because of their viral spread online."[7] Making things worse, this extremist content often boomerangs from fringe websites to mainstream platforms—in part because of social media's immense power, amplification of "engaging" content, and sophisticated recommendation engines, all working together to underpin a business model reliant on surveillance advertising.[8]

It is important to note that extremism and hate that start on social media do not always stay there. This content has inspired individuals to commit acts of violence and domestic terrorism.[9] Only a few months ago, an 18-year-old who espoused white supremacist and antisemitic views online organized and live-streamed via Twitch a shooting rampage that left ten people dead in a predominantly Black neighborhood in Buffalo. The footage of the shooting was later boomeranged from fringe websites to mainstream platforms, remaining online for days.[10]

[4] Bidar, Musadiq. *Facebook researchers saw how its algorithms led to misinformation.* (2021, October 25) CBSNews. https://www.cbsnews.com/news/facebook-algorithm-news-feed-conservatives-liberals-india/

[5] Isaac, Mike. *Facebook Wrestles with the Features It Used to Define Social Networking.* NY Times. (2021, Oct 25).

[6] Egan, Matt. Anti-Defamation League CEO on Facebook: Never has a single company been responsible for so much misfortune. CNN. (2021, October 25). https://edition.cnn.com/2021/10/25/business/facebook-leak-papers-adl

[7] Greenblatt, Jonathan. *Congressional Testimony: Holding Big Tech Accountable: Legislation to Build a Safer Internet.* (2021, December 09). House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce.
https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Greenblatt_CPC_2021.12.09_1.pdf

[8] *For Twitter Users, Gab's Toxic Content Is Just a Click Away*. (2021, October 11). ADL. https://www.adl.org/blog/for-twitter-users-gabs-toxic-content-is-just-a-click-away

[9] *Gab and 8chan: Home to Terrorist Plots Hiding in Plain Sight*. (2018). ADL. https://www.adl.org/resources/reports/gab-and-8chan-home-to-terrorist-plots-hiding-in-plain-sight

[10] *Footage of Buffalo Attack Spread Quickly Across Platforms, Has Been Online for Days.* (2022, May 24). ADL. https://www.adl.org/resources/blog/footage-buffalo-attack-spread-quickly-across-platforms-has-been-online-days

The offline consequences of online hate and extremism continue to be documented in an ever-increasing record of harm that has yet to result in effective remedies from tech companies. Moreover, an expanding body of research has shown that the consequences of amplifying hate and otherwise providing incentives for engaging with once-fringe conspiracy theories do not merely reflect real-world trends, they create new ones. That is, as a result of the decision to maximize engagement as the sole or overarching metric of any significance, the platforms are radicalizing increasing numbers of users and creating new communities of extremists and conspiracists.[11] The surveillance advertising/maximize engagement business model thus has enormous reality- and behavior-distorting effects.[12]

Of particular note is the threat that tech companies' collection and exploitation at scale of personal data for commercial purposes poses to vulnerable and marginalized communities, especially people of color, women, religious minorities, and members of the LGBTQ+ community. There are at least two mechanisms at play:

1. *The surveillance-based advertising business model rewards extreme, hateful, and polarizing content. Individuals experience alarming rates of identity-based harassment.*

As observed, research shows that controversial, hateful, and polarizing information and misinformation are often more engaging than other types of content and, therefore, receive wider circulation.[13] Or put another way, a model of serving up content that is based on the goal of maximizing engagement–which is what grows revenue–actually increases polarization. The real world effects are alarming. For example, surveillance-based ads and their microtargeting capabilities are often exploited by both commercial and non-commercial advertisers to suppress the vote of marginalized and underrepresented communities, recruit and radicalize susceptible individuals, discriminate in economic opportunities or the exercise of rights, and promote goods that could endanger the physical safety of vulnerable users.[14]

Despite tech companies' public commitments to improving safety on their platform, online harassment is an extremely common occurrence. ADL's 2022 Online Hate and Harassment Survey[15] revealed that 2 in 5 Americans (40%) experienced some type of online harassment in the course of their lives, with 1 in 10 (12%) having experienced severe types of harassment—defined as including physical threats, sustained harassment, stalking, sexual harassment, doxing,

[11] Zadrozny, Brandy. *"Carol's Journey": What Facebook Knew about How It Radicalized Users*. NBC News. (2021, October 22). https://www.nbcnews.com/tech/tech-news/facebook-knew-radicalized-users-rcna3581

[12] Fisher, Max. *The Chaos Machine: The Inside Story of How Social Media Rewired Our Minds and Our World*. Little, Brown and Company, 2022

[13] *How Algorithms Influence Harmful Online Conduct.* (2021, September). ADL. https://committees.parliament.uk/writtenevidence/39113/html/

[14] Rabkin, Job et. al. *Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016*. Channel 4. (2020, September 28). https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016; Angwin, Julia et. al. *Facebook enabled advertisers to reach 'Jew Haters',* ProPublica, (2017, September 14). https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters; Merrill, Jeremy. *Google has been allowing advertisers to exclude nonbinary people from seeing job ads*, The Markup, (2021, February 11). https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads; *How Facebook profits from the insurrection,* Tech Transparency Project, (2021, January 18). https://www.techtransparencyproject.org/articles/how-facebook-profits-insurrection

[15] *Online Hate and Harassment: The American Experience 2022*. (2022, June). ADL. https://www.adl.org/sites/default/files/pdfs/2022-07/Online-Hate-and-Harassment--Survey-2022.pdf

and/or swatting—in the past 12 months. Data from the same survey also shows that marginalized or minoritized identity groups—including Jews, women, people of color, and LGBTQ+ people—experience hate-based online harassment (i.e., targeted attacks or abuse of marginalized people because of their race, ethnicity, religion, gender, sexuality, physical appearance, gender, identity, or disability) at disproportionately high levels. According to the study, 65% of people from these groups who experienced online harassment reported being targeted for an aspect of their identity, compared to 38% of people from non-marginalized groups. Moreover, in addition to severe harassment for historically marginalized groups being higher, these groups also experienced higher rates of online stalking (12% vs. 6%) and sexual harassment (12% vs. 5%).

In addition, the study reveals identity-specific differences in the incidence of harassment, its growth trend, and the type of abuse endured. In particular:

- LGBTQ+ people are more likely than any other marginalized group to experience online harassment: 66% of LGBTQ+ users surveyed experienced harassment compared to 38% of non-LGBTQ+, with 1 in 2 (53%) attributing the targeting to their sexual orientation.
- Asian Americans reported the most significant increase in online harassment in the last two years (from 11% in 2020 to 39% in 2022), tracking closely with the rise in anti-Asian incidents offline. Furthermore, 62% attributed the harassment to their physical appearance and 53% to their race or ethnicity, compared to 34% and 23% of non-Asian Americans.
- Women were more than twice as likely to report ever experiencing sexual harassment online as men were (14% vs. 5%), with 2 in 5 attributing the harassment to their gender (vs. 1 in 7 of men). The intersectionality matrix also seems to be at play, with 81% of non-white women attributing being harassed to aspects of their identity (vs. 61% of white women).
- Although Jewish respondents experienced online harassment at similar rates as non-Jews, they were more likely to attribute harassment to their religion (37% vs. 14%).

According to the same survey, youth–especially marginalized–are at particular risk of experiencing online harassment across all platforms. Nearly half of respondents (47%) ages 13-17 experienced online harassment at some point in their lives, with one-fourth (25%) experiencing severe harassment. Teens also experienced hate-based harassment at a higher rate than adults.

An overwhelming majority of respondents who experienced harassment said that the abuse happened on Facebook (68%), with Instagram, Twitter, and YouTube following far behind (26%, 23%, and 20%, respectively). Similar trends were also observed in the last 12 months. Notably, Facebook's primacy holds even when accounting for the proportion of platform users compared to the proportion of those who reported harassment on the platform.

To a large extent, many tech platforms' role in enabling and amplifying online harassment can be explained by a business model that optimizes for user engagement and the company's overreliance on algorithmic AI/ML systems to moderate content. First, AI and ML-based tools deployed to moderate content do not do well assessing context and make subjective decisions, allowing a significant amount of harmful content to go undetected.[16] Second, as hateful, harassing content often has high engagement rates, when this content evades detection from content moderation systems, it is spread and amplified by platforms' ranking and recommendation algorithms faster than other types of content.[17]

Separate from the fundamental role of the AI and ML-based tools, it is also worth noting that even when presented with extensive evidence of the presence and amplification of hate and harassment on its platforms, Meta, like other big platforms, has been slow to remove or otherwise mitigate that content or the functions that spread it.[18]

2. *Surveillance-based ads are often used by advertisers as a tool for discrimination, manipulation, and oppression against specific identities.*

Social media companies collect massive troves of user data to ensure that the advertisements the platforms deliver are highly targeted to users.[19] As digital ads are relatively cheap, advertisers can also test their messages multiple times and refine them to achieve the greatest impact. The more data available for each user, the greater the ability to segment the customer base and customize messages.

While microtargeting tools can help small companies and political challengers level the playing field to their advantage, they can also be used by both commercial and non-commercial advertisers as a tool for discrimination, manipulation, and oppression against marginalized and minoritized identities. In the last few years, journalists and watchdogs uncovered countless examples of how digital ads can be at the service of hate and extremism against the Jewish people, members of the LGBTQ+ community, women, immigrants, people of color, and other historically targeted communities:

- Digital ads can enable voter suppression efforts against marginalized and underrepresented communities. For example, former President Trump's campaign used personal information secretly harvested from Facebook to profile, categorize voters, and target them with personalized digital ads ahead of the 2016 presidential election.[20] As a

[16] *Trained for Deception: How Artificial Intelligence Fuels Online Disinformation.* (2021, September). The Coalition to Fight Digital Deception. https://assets.mofoprod.net/network/documents/Trained_for_Deception_How_Artificial_Intelligence_Fuels_Online_Disinformation_T2pk9Wj.pdf

[17] *How Algorithms Influence Harmful Online Conduct.* (2021, September). ADL. https://committees.parliament.uk/writtenevidence/39113/html/

[18] *What Will Finally be the Tipping Point Against Facebook.* (2021, September 27). ADL. https://www.adl.org/blog/what-will-finally-be-the-tipping-point-against-facebook

[19] Greenblatt, Jonathan. *Congressional Testimony: Holding Big Tech Accountable: Legislation to Build a Safer Internet.* (2021, December 09). House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce. https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Greenblatt_CPC_2021.12.09_1.pdf

[20] Rosenberg, Matthew et. al. *How Trump Consultants Exploited the Facebook Data of Millions.* (2018, March 17). NYTimes. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

result, millions of Black Americans were targeted with manipulative messages aimed to discourage them from voting.[21]

- Hate groups can use digital ads to recruit and radicalize susceptible individuals. As unveiled by ProPublica, Facebook allowed advertisers to target users who previously expressed interest in topics such as "Jew hater," "How to burn Jews," or "History of 'why Jews ruin the world."[22]
- Digital ads can be used to discriminate in economic opportunities. As uncovered by The Markup, dozens of advertisers used Google's ad targeting capabilities to exclude–inadvertently or purposefully–people who identify as nonbinary, transgender, or anything other than male or female from seeing housing, credit, or job ads.[23]
- Digital ads can increase the likelihood of physical harm. According to research by the Tech Transparency Project, Facebook recklessly served ads for weapons accessories and body armor next to inflammatory discussions in militia and "patriot" groups on the platform, even after the January 6, 2021 Capitol attack in Washington.[24]

3. *Online multiplayer gaming spaces also host alarming rates of identity-based harassment.*

Online multiplayer games, which are played by close to 100 million Americans, expose users to an increased risk of online hate and harassment, as confirmed by ADL's annual report on experiences in online games.[25] While there is limited data on how video game companies are surveilling their players in-game, there have been reports about an increase in middleware "data analytics" tools.[26] In light of this trend, it is crucial for us to be ahead of the curve when it comes to tracking surveillance advertising in online games spaces.

For the third consecutive year, an ADL survey on American gamers found that harassment experienced by adult gamers is both alarmingly high and on the rise. Not only 5 out of 6 adults (83%) ages 18-45 experienced harassment in online multiplayer games, but 71% experienced severe abuse, including physical threats, stalking, and sustained harassment. Furthermore, the same survey shows that the most significant increases in identity-based harassment occurred among respondents who identified as women (49% in 2021, compared to 41% in 2020), Black or African American (42% in 2021, compared to 31% in 2020), and Asian American (38% in 2021,

[21] Rabkin, Job et. al. *Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016.* (2020, September 28). Channel4. https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016

[22] Angwin, Julia et. al. *Facebook Enabled Advertisers to Reach 'Jew Haters'.* (2017, September 14). ProPublica. https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters

[23] Merrill, Jeremy. *Google Has Been Allowing Advertisers to Exclude Nonbinary People from Seeing Job Ads.* (2021, February 11). The Markup. https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads

[24] *How Facebook Profits from the Insurrection.* (2021, January 18). Tech Transparency Project. https://www.techtransparencyproject.org/articles/how-facebook-profits-insurrection

[25] *Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021*. (2022, May 3). ADL. https://www.adl.org/hateisnogame

[26] Egliston, Ben. *The Unnerving Rise of Video Games that Spy on You*. (2022, February 1). Wired. https://www.wired.com/story/video-games-data-privacy-artificial-intelligence/; Bernevega, A. et al. *The Industry of Landlords: Exploring the Assetization of the Triple-A Game.* (2022). Games and Culture, 17(1), 47–69. https://doi.org/10.1177/15554120211014151

compared to 26% in 2020). Although LGBTQ+ players did not experience a significant rise in the amount of harassment experiences (38% in 2021 versus 37% in 2020), the share of LGBTQ+ respondents experiencing harassment in online multiplayer games is still of concern.[27]

Data collected by ADL also confirms that young gamers are more likely to be the target of online harassment than adults. In particular, 3 in 5 respondents ages 13-17 experienced harassment in online multiplayer games, despite a vast majority of young gamers also reporting some form of positive social experience. Similarly to adult gamers, identity-based harassment was a problem for young gamers who identified as Black or African American, women, and Asian American.[28]

Proposals for Protecting Consumers from Harmful and Prevalent Commercial Surveillance

ADL has consistently stated that holding social media companies accountable for fomenting violence, disinformation, and other forms of hate leading to harm will require a multipronged approach that includes increased transparency, oversight, and targeted reform of the near-blanket legal immunity afforded platforms by Section 230 of the Communications Decency Act–in this last case, reform that prioritizes civil rights and civil liberties concerns without impinging on free speech, discouraging helpful content moderation, or solidifying Big Tech's market power. ADL's REPAIR Plan presents a comprehensive agenda to push hate and extremism to the fringes of the digital world.[29] Among them, regulating the collection and use of personal data in a way that prioritizes people over profit would go a long way in protecting vulnerable and marginalized individuals from online abuse enabled by social media's exploitation of personal data. In particular, ADL invites the Commission to consider the following proposals.

1. *Ban Surveillance Advertising.*

Social media companies make money by surveilling our behavior, collecting our data, and tweaking their algorithms to amplify and recommend content that will keep users online for as long as possible—so they can specifically target those users with as many advertisements as possible. Under this business model, hate, violence, and misinformation thrive because, as ample research has shown, that type of content gets engagement. The surveillance advertising business model encourages social media companies to profit from people's propensity to click on incendiary content and share and otherwise engage with extremist content and misinformation. ADL urges the FTC to take seriously the extraordinary role surveillance advertising plays in mainstreaming and normalizing hate and extremism and the threat posed to vulnerable communities and democratic processes and institutions. The current mainstreaming of extremism, and accompanying threats of violence, depend in significant part upon the amplification social media platforms afford such ideologies, movements and groups.

We ask the FTC to give meaningful consideration to Accountable Tech's Petition for

[27] *Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021*. (2022, May 3). ADL. https://www.adl.org/hateisnogame

[28] *Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021.* (2022, May 3). ADL. https://www.adl.org/hateisnogame

[29] *REPAIR Plan: Fighting Hate in the Digital World.* ADL. https://www.adl.org/repairplan

Rulemaking to Prohibit Surveillance Advertising.[30] If not immediately feasible, the Commission should at least prohibit surveillance-based advertising to any individuals under 17, provide any other users with the ability to opt-out of targeted advertising, and plan for a gradual phase-out leading to a prohibition of targeted advertising based on personal data.

2. *Prohibit the collection, processing, or transferring to a third party of sensitive data without a user's affirmative consent.*

Currently, there are no legal limits to the amount or types of data that digital platforms can collect or use to target users, including sensitive data such as race, ethnicity, religion, national origin, sexual orientation, gender identity, and more. Although social media companies have gradually limited the range and scope of personal data that advertisers can use to target their audience, leaving the protection of user privacy subject to the whims of tech executives can have dangerous consequences. For example, using data from its Citizen Browser, The Markup found that advertisers still can and do target Facebook's users based on proxies for sensitive categories,[31] despite the company's pledge to remove "sensitive" categories such as race, health conditions, and political affiliation from ad-targeting options.[32]

Hoarding sensitive data can disproportionately affect historically targeted individuals and communities, endangering their emotional and/or physical safety. To prevent the abuse of personal data as a tool for discrimination, manipulation, and oppression, ADL asks the FTC to consider a prohibition on the collection, processing, or transfer to a third party of a user's sensitive data—e.g., information revealing race, ethnicity, national origin, religion, sexual orientation; recordings maintained for private use in a device; information revealing online activities over time and across third-party services—without their express affirmative consent. The FTC's own reporting revealed how technology companies use "dark patterns" (sophisticated design practices that manipulate consumers into giving up their personal data) to profit off of unsuspecting users.[33] This practice does not prioritize consumer protection. Consumers should not have to decipher cryptic terms of service to protect their personal information from being exploited in the name of data monetization.

3. *Impose a data minimization requirement.*

To reduce the risks of social media's lax data security practices, ADL invites the FTC to consider adopting a data minimization requirement by mandating that the collection, use, and retention of data be limited to what is reasonably necessary or required to provide the service requested by the consumer rather than collecting as much data as possible to perpetuate targeted ads that so often spread disinformation and hate. This is needed to combat extremism, which has

[30] *Re: Petition for Rulemaking to Prohibit Surveillance Advertising*. (2022). Accountable Tech. https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf

[31] Waller, Angie and Lecher, Colin. *Facebook Promised to Remove "Sensitive" Ads. Here's What It Left Behind.* (2020, May 12). The Markup. https://themarkup.org/newsletter/citizen-browser/facebook-promised-to-remove-sensitive-ads-heres-what-it-left-behind

[32] Milmo, Dan. *Facebook bans ads targeting race, sexual orientation and religion.* (2021, November 10). The Guardian. https://www.theguardian.com/technology/2021/nov/10/facebook-bans-ads-targeting-race-sexual-orientation-and-religion

[33] *FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers*. (2022, September 15). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers

increased in reach and influence as a result of commercial surveillance practices. In fact, in an October 2021 study, ADL's Center on Extremism found that despite Twitter's ban on external links to hate speech, extremist material, and conspiracy theories, this content is frequently shared on Twitter via links from far-right sites.[34] It was in an effort to combat online hate such as this that led ADL to launch the Center for Technology and Society (CTS) in 2017.[35] CTS has studied this area and, in direct engagement with platforms, among other things, has emphasized the need for them to adopt anti-hate-by-design principles and functionalities to build less hate-filled platforms.[36]

4. *Require Platforms to Set Users' Privacy Settings to the Most Secure by Default.*

The FTC should also require platforms to set users' privacy settings to the most secure by default, to help mitigate breaches of sensitive information, such as geolocation, biometric information, and the like that are often used to perpetuate digital abuse and cybercrimes. Bad actors utilize sensitive information to harass and harm others through doxing and swatting, which have led to harmful–even fatal–outcomes. Bad actors often go as far as to purchase information from others.[37] In an effort to fight online hate and harassment, ADL launched the Backspace Hate initiative to support victims and targets of online hate and harassment by raising awareness and passing legislation to better hold perpetrators accountable for their actions online.[38] We urge the FTC to implement rules to improve data security to help mitigate harm.

5. *Require platforms to implement user-controlled, easily accessed privacy settings.*

Data from ADL's 2022 Online Hate and Harassment Survey clearly shows that marginalized or minoritized identity groups on social platforms are more susceptible to being targeted by harassers.[39] This finding also holds true for online gamers. To protect them, ADL urges the Commission to require platforms to enable users to easily access and change the privacy settings of their account, and allow them to hide their information and content from other users, including options such as "public," "followers only," "followers of followers."[40]

As discussed by CTS in its Anti-Hate by Design social pattern library, giving users the option to choose who can see their content would have several benefits, including maintaining privacy in the case that they are being harassed, mitigating the risk of harassers finding their content and targeting them, or tackling network or campaign harassment before it begins.[41] If the account

[34] *For Twitter Users, Gab's Toxic Content Is Just a Click Away*. (2021, October 11). ADL. https://www.adl.org/blog/for-twitter-users-gabs-toxic-content-is-just-a-click-away

[35] *Center for Technology & Society.* (2017). ADL. https://www.adl.org/research-centers/center-technology-society

[36] Sifry, David. *Congressional Testimony: Social Media Platforms and the Amplification of Domestic Extremism & Other Harmful Content.* (2021, October 9). ADL. https://www.adl.org/sites/default/files/adl-testimony-house-homeland-security-social-media-domestic-extremism-2021-10-28.pdf

[37] Suciu, Peter. *Social Media User Information For Sale On The Dark Web*. (2022, July 27). Forbes. https://www.forbes.com/sites/petersuciu/2022/07/27/social-media-user-information-for-sale-on-the-dark-web/?sh=2f2dca8b7111

[38] *Backspace Hate*. ADL. https://www.adl.org/backspace-hate

[39] *Online Hate and Harassment: The American Experience 2022*. (2022, June). ADL. https://www.adl.org/sites/default/files/pdfs/2022-07/Online-Hate-and-Harassment--Survey-2022.pdf

[40] *Account Privacy Setting.* ADL. https://socialpatterns.adl.org/patterns/account-privacy-setting/

[41] *Social Pattern Library.* ADL. https://socialpatterns.adl.org/

privacy is set to hide from public viewing, this pattern can also make it difficult for harassers to find users' information and harass them on other platforms (e.g., gaming platforms), or potentially off-platform if they are able to locate users.

6. *Require multiplayer VR platforms to provide better protection to users.*

ADL Report "Hate in Social VR" extensively discusses how virtual reality (VR) platforms' users can be exposed to harassment through their avatars.[42] "Virtual reality and augmented reality present exceedingly complex privacy issues because of the enhanced user experience and reality-based models."[43] With VR offerings expected to boom, the FTC should adopt a preventive approach and require multiplayer virtual reality platforms that provide users the ability to interact physically with one another to give them the option to create a buffer zone free from harassment. These settings could be configured by users. This privacy setting option is detailed in CTS' Anti-Hate by Design social pattern library, and would go a long way in mitigating inappropriate VR interactions with other users.[44]

In summary, ADL urges the FTC to make the impact that surveillance advertising and the hoarding of personal data has on mainstreaming and normalizing hateful and extremist content a significant factor in support of a decision to adopt R111004. The type of content spread virally by platforms as a result of their reliance upon a surveillance advertising business model has inspired people to target individuals and communities online and commit acts of violence offline. The harm to individuals, vulnerable communities, and democratic processes in this country and their relationship to online extremism and radicalization are well-documented and are only growing. We are hopeful that the Commission will produce a final rule that decreases the proliferation of hate and extremism, protects civil rights, reduces harm to consumers, promotes competition, and protects our democracy. We know that it will take more than one rulemaking to comprehensively address hate and extremism online; however, the Commission's actions here are necessary as a first step.

We thank the FTC for their vital work and look forward to reviewing the proposed rule. We would be honored to testify on this subject if hearings are held.

Sincerely,

Max Sevillia
Vice President for Government Relations, Advocacy and Community Engagement
ADL (Anti-Defamation League)

[42] *Hate in Social VR.* (2018, July 12). ADL. https://www.adl.org/resources/reports/hate-in-social-virtual-reality

[43] Heller, Brittan. *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*. 23 Vanderbilt Journal of Entertainment and Technology Law 1 (2021). https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1; D'Anastasio, Cecilia et al. *The Creators Of Pokémon Go Mapped The World. Now They're Mapping You.* (2019, October 16). Kotaku. https://kotaku.com/the-creators-of-pokemon-go-mapped-the-world-now-theyre-1838974714

[44] *Personal Bubble Setting.* ADL. https://socialpatterns.adl.org/patterns/personal-bubble-setting/