

From: Moore, Robin
Sent: Tue, 23 Mar 2021 20:08:57 +0000
To: Kopec, Janice; King, Austin; Perkins, Rhonda
Cc: Kaufman, Daniel
Subject: [REDACTED]
Attachments: [REDACTED]

Janice, Austin, Rhonda –

[REDACTED]

We look forward to your thoughts.

Best,
Robin

Robin L. Moore
Acting Chief of Staff
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, NW,
Washington, DC 20580
(202) 326-2167

[REDACTED]

From: Zylberglait, Pablo
Sent: Thu, 2 Dec 2021 13:37:47 +0000
To: Kalepe, Roland
Cc: Batal, Mohamad; Bumpus, Jeanne; Christie, Joel; Coppola, Maria; Crawford, Molly; Delaney, Elizabeth A; Dolan, Reilly; Estrada, Danielle; Freer, Daniel R.; Gorman, Frank; Howard, Jennifer; Kaplan, Peter P.; King, Austin; Kopec, Janice; Koulousias, Amanda; Kryzak, Lindsay; Laroia, Gaurav; Levine, Samuel; Lezaja, Michael; Liu, Josephine; Moore, Robin; Perkins, Rhonda; Pesin, Michael; Runco, Philip; Simons, Claudia A.; Spector, Robin; Tabor, April; Vaca, Monica E.; Vandecar, Kim; Wayne, Catherine; White, Katherine; Zhao, Daniel
Subject: (b)(5) Letter from Rep. Crist re: Spanish-language content moderation
Attachments: Crist FTC Spanish Misinformation.pdf

Hi Roland,

Please assign this (b)(5) letter as follows:

From	To	Regarding	Commission approval	Deadline	Who signs	Link
Rep. Crist	BCP (Robin Moore)	Spanish-language content moderation	No	Wednesday, December 22, 2021	Chair Khan	(b)(5); (b)(3)-FISMA 44 USC 3555(f)

Thanks,

Pablo

CHARLIE CRIST
13TH DISTRICT, FLORIDA
www.crist.house.gov

215 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-5961

696 1ST AVENUE NORTH, SUITE 203
ST. PETERSBURG, FL 33701
(727) 318-6770

Congress of the United States
House of Representatives
Washington, DC 20515-0913

APPROPRIATIONS COMMITTEE
SUBCOMMITTEES:
DEFENSE
COMMERCE, JUSTICE, SCIENCE
MILITARY CONSTRUCTION, VETERANS
AFFAIRS AND RELATED AGENCIES
SCIENCE, SPACE, AND
TECHNOLOGY COMMITTEE
SUBCOMMITTEES:
SPACE AND AERONAUTICS
ENVIRONMENT

December 1, 2021

The Honorable Lina Khan, Chair
Federal Trade Commission
600 Pennsylvania Ave, N.W.
Washington, D.C. 20580

Dear Chair Khan,

I write to you to today to highlight an October 28th article in the *Washington Post* titled "Misinformation online is bad in English. But it's far worse in Spanish."¹ I have been concerned for some time about the spread of misinformation online but was especially disturbed to read that Spanish-language posts are less moderated and left up longer than those in English.

As with any problem, it is crucial to start with the facts. Unfortunately, there is simply a dearth of data related to Spanish-language content moderation online. As it stands now, policymakers are left to rely on statements from social media platforms on their content moderation practices and testimony from whistleblowers like Frances Hauge. Sadly, those only pertain to content in English. Additional data is needed to understand the scope of the problem and how to tackle it.

As you know, Section 6(b) of the Federal Trade Commission Act empowers the FTC to require companies to file "reports or answers in writing to specific questions" about its business practices – as the FTC did with Amazon, TikTok, Facebook, Reddit, Snap, Twitter, WhatsApp, and YouTube in December 2020. Additionally, in April of this year, FTC Acting Chairwoman Rebecca Kelly Slaughter testified before Congress on the agency's recent enforcement actions, including filing more than a dozen law enforcement cases against individuals who participated in selling fraudulent COVID products. I applaud these initial efforts and ask that the FTC redouble its inquires, specifically as it pertains to misinformation in Spanish-language content online and in radio and television advertising.

In addition, it would be instructive to know specific metrics on how many Spanish-language posts were flagged or taken down compared to posts in English, and how many Spanish-speaking content moderators are employed at each of the above listed social media companies. Given the lack of information on Spanish-language content moderation, I am requesting the FTC compile this information and provide it to Congress, as it would prove useful for either future enforcement or legislation to safeguard families from misinformation.

I thank you again for all of your efforts to date and look forward to receiving the data you compile so that we can work together to combat the scourge of misinformation.

Sincerely,



Charlie Crist
UNITED STATES CONGRESSMAN

¹ <https://www.washingtonpost.com/outlook/2021/10/28/misinformation-spanish-facebook-social-media/>

From: King, Austin (he/him)
Sent: Thu, 16 Mar 2023 08:48:09 +0000
To: Slaughter, Rebecca
Subject: RE: Bullets on OCM items
Attachments: [redacted] (b)(5)

[redacted] (b)(5)

[redacted] (b)(5)

From: King, Austin (he/him)
Sent: Wednesday, March 15, 2023 5:07 PM
To: Slaughter, Rebecca <rslaughter@ftc.gov>
Cc: Laroia, Gaurav <glaroia@ftc.gov>
Subject: Bullets on OCM items

Hi, Becca:

[redacted] (b)(5)

(b)(5)

Thanks!
Austin

From: Kopec, Janice
Sent: Wed, 1 Jun 2022 18:23:05 +0000
To: Slaughter, Rebecca

Subject: [redacted] (b)(5)

Attachments: [redacted] (b)(5)

[redacted] (b)(5)

[redacted] (b)(5)

From: Kopec, Janice
Sent: Tuesday, May 24, 2022 7:01 PM
To: Slaughter, Rebecca <rslaughter@ftc.gov>

Subject: [redacted] (b)(5)

[redacted] (b)(5)

From: Kopec, Janice
Sent: Mon, 17 May 2021 21:43:26 +0000
To: Slaughter, Rebecca
Subject: FW: Final Review: Needed Resources and Overview
Attachments: DRAFT-FY22 CBJ Needed Resources_Overview_20210517.docx

(b)(5)

From: Hale, James <jhale@ftc.gov>
Sent: Monday, May 17, 2021 4:59 PM
To: Kopec, Janice <jkopec@ftc.gov>
Cc: Rebich, David <drebich@ftc.gov>; Walsh-Van Wey, Lori <lwalshvanwey@ftc.gov>
Subject: Final Review: Needed Resources and Overview

(b)(5)

Let me know if you have any questions.

Many thanks,
James

From: Batal, Mohamad
Sent: Fri, 6 May 2022 20:59:22 +0000
To: Slaughter, Rebecca; Kopec, Janice; Laroia, Gaurav
Subject: FW:(b)(5) letter from Reps. Butterfield, Aguilar, and Leger Fernandez re: bots and fake accounts affecting elections
Attachments: FTC Letter.pdf

Hey Becca—Please see the attached (b)(5) letter about bots, fake accounts, and elections.

Thanks,
 Moh

From: Zylberglait, Pablo <PZYLBERGLAIT@ftc.gov>
Sent: Friday, May 6, 2022 8:40 AM
To: Kalepe, Roland <rkalepe@ftc.gov>
Cc: Alan, Laura <lalan@ftc.gov>; Batal, Mohamad <mbatal@ftc.gov>; Bumpus, Jeanne <JBumpus@ftc.gov>; Christie, Joel <JCHRISTIE@ftc.gov>; Coppola, Maria <mcoppola@ftc.gov>; Crawford, Molly <mcrawford@ftc.gov>; Dasgupta, Anisha <adasgupta@ftc.gov>; Delaney, Elizabeth A <EDELANEY@ftc.gov>; Dolan, Reilly <JDOLAN@ftc.gov>; Estrada, Danielle <destrada@ftc.gov>; Freer, Daniel R. <dfreer@ftc.gov>; Howard, Jennifer <jhoward1@ftc.gov>; Kaplan, Peter P. <pkaplan@ftc.gov>; King, Austin (he/him) <aking3@ftc.gov>; Kopec, Janice <jkopec@ftc.gov>; Koulousias, Amanda <akoulousias@ftc.gov>; Laroia, Gaurav <glaroia@ftc.gov>; Levine, Samuel <slevine1@ftc.gov>; Lezaja, Michael <mlezaja@ftc.gov>; Liu, Josephine <jliu1@ftc.gov>; Moore, Robin <rmoore@ftc.gov>; Perkins, Rhonda <rperkins@ftc.gov>; Robinson, Carolyn L. <crobinson@ftc.gov>; Runco, Philip <prunco@ftc.gov>; Simons, Claudia A. <CSIMONS@ftc.gov>; Spector, Robin <rspector@ftc.gov>; Tabor, April <atabor@ftc.gov>; Unruh, Rebecca <runruh@ftc.gov>; Vaca, Monica E. <MVACA@ftc.gov>; Vandecar, Kim <KVANDECAR@ftc.gov>; Wayne, Catherine <cwayne@ftc.gov>; White, Katherine <kwhite@ftc.gov>; Wilson, Christine <cwilson3@ftc.gov>; Zhao, Daniel <dzhao@ftc.gov>
Subject: (b)(5) letter from Reps. Butterfield, Aguilar, and Leger Fernandez re: bots and fake accounts affecting elections

Hi Roland,

Please assign this (b)(5) letter as follows:

From	To	Regarding	Commission approval	Deadline	Who signs	Link
Reps. Butterfield, Aguilar, and Leger Fernandez	BCP (Robin Moore)	Use of bots and fake accounts, particularly as they relate to	No	Thursday, May 26, 2022	Chair Khan	(b)(5); (b)(3): FISMA 44 USC 3555(f)

		federal elections.				
--	--	-----------------------	--	--	--	--

Thanks,

Pablo

ZOE LOFGREN, CALIFORNIA
CHAIRPERSON

JAMIE RASKIN, MARYLAND
G.K. BUTTERFIELD, NORTH CAROLINA
PETE AGUILAR, CALIFORNIA
MARY GAY SCANLON, PENNSYLVANIA
VICE CHAIRPERSON
TERESA LEGER FERNANDEZ, NEW MEXICO

JAMIE FLEET
STAFF DIRECTOR

One Hundred Seventeenth
Congress of the United States
House of Representatives

COMMITTEE ON HOUSE ADMINISTRATION

1309 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6157
202-225-2061 | CHA.HOUSE.GOV

RODNEY DAVIS, ILLINOIS
RANKING MINORITY MEMBER

BARRY LOUDERMILK, GEORGIA
BRYAN STEIL, WISCONSIN

TIM MONAHAN
MINORITY STAFF DIRECTOR

May 5, 2022

Lina Khan
Chairperson
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Chairperson Khan:

As members of the Committee on House Administration Subcommittee on Elections, we are concerned about the use of fake and automated accounts, known as bots, to disseminate election-related mis- and disinformation on social media platforms. Indeed, a study conducted by the University of Southern California during the lead up to the 2020 election found that thousands of bots were posting about the two presidential candidates and their campaigns on Twitter. The study found that the bots “exacerbate the consumption of the content within the same political chamber, so it increases the effect of the echo chamber.”¹ Moreover, an internal Facebook memo written in March 2021 revealed the company’s ability to detect anti-vaccine rhetoric and misinformation was “basically non-existent” in non-English comments.² Frances Haugen, a former Facebook employee turned whistleblower, said that the company spends 87 percent of its misinformation budget on U.S. content.³

The Federal Trade Commission has an opportunity to exercise its authority to address some of the market issues related to bots and fake accounts, particularly those with a nexus to federal elections. Several proposals were contained in a July 16, 2020, statement, “Regarding the Report to Congress on Social Media Bots and Deceptive Advertising Commission File No. P204503,” from former Commissioner Rohit Chopra.⁴

¹ Emily Gersema, *Election 2020 chatter on Twitter busy with bots and conspiracy theorists*, USC NEWS (Oct. 28, 2020), available at <https://news.usc.edu/177963/election-2020-twitter-social-media-bots-foreign-interference-usc-study/>

² Amanda Seitz and Will Weissert, *Inside the ‘big wave’ of misinformation targeted at Latinos in Florida, elsewhere*, ORLANDO SENTINEL (Nov. 29, 2021), <https://www.orlandosentinel.com/politics/os-ne-inside-the-big-wave-of-misinformation-targeted-at-latinos-20211129-arlx66zghbavtg2my4hutqj44u-story.html>.

³ *Id.* An analysis done by online activist group Avaaz, found that Facebook failed to flag 70 percent of Spanish-language misinformation surrounding COVID-19 compared to just 29 percent of such information in English. *Id.*

⁴ Statement of Commissioner Rohit Chopra, “Regarding the Report to Congress on Social Media Bots and Deceptive Advertising Commission File No. P204503,” July 16, 2020, available at https://www.ftc.gov/system/files/documents/public_statements/1578231/social_bots_chopra_statement.pdf.

We are interested to learn whether the Commission has considered exercising the authority outlined by former Commissioner Chopra. Specifically, we would like the Commission to answer the enclosed questions.

Thank you in advance for your assistance with this matter. We respectfully request your responses by May 20, 2022. If you have any questions regarding this request, please contact Committee staff at (202) 225-2061.

Sincerely,



G. K. Butterfield
Chair
Subcommittee on Elections



Pete Aguilar
Member
Subcommittee on Elections



Teresa Leger Fernández
Member
Subcommittee on Elections

cc: The Honorable Zoe Lofgren, Chairperson
Committee on House Administration

The Honorable Darren Soto
Member of Congress, Florida's 9th Congressional District

The Honorable Nanette Barragán
Member of Congress, California's 44th Congressional District

QUESTIONS

1. Has the Commission studied, or does it plan on studying, the impact that bots and fake accounts have on political advertisements, including advertisements by candidates, elected officials, and issue-based political organizations, on social media platforms? If so, please provide details on any studies or actions you have undertaken.

2. One of the ways social media platforms generate revenue is through digital advertising on their platforms. Platforms provide to advertisers information about the potential reach and engagement of advertisements on their platform, as well as impression data for any given ad. In addition to impacting the spread of election-related disinformation, bots and fake accounts can also artificially inflate engagement and impression data. If platforms are providing false or unsubstantiated information, for example, impression data inflated by bots, that could potentially be a violation of the Federal Trade Commission Act's prohibition on deceptive acts or practices.
 - a. Has the Commission considered using its authority under the Act to assess the validity of social media companies claims to advertisers about potential reach and engagement of advertisements on their platform?

 - b. Has the Commission considered using its authority under the Act to assess the validity of social media companies claims regarding the impression data of advertisements on their platforms?

3. The sale of fake followers can influence the spread of disinformation on social media platforms by increasing the perceived influence of individuals promoting false information. In 2019, the Commission announced an enforcement action against Devumi, which was "a company that sold fake subscribers, views, and likes, to people trying to artificially inflate their social media presence."⁵ Since that enforcement action, what work has the Commission done to deter companies selling fake followers?

4. Election related disinformation is not just spreading in English, it is also being shared to a wide audience in languages other than English. What has the Commission done to study the existence and impact of social media bots and fake accounts that interact with posts or post in languages other than English?

⁵ Federal Trade Commission Report to Congress, "Social Media Bots and Deceptive Advertising," July 16, 2020.

From: Laroia, Gaurav
Sent: Thu, 29 Jul 2021 16:01:40 +0000
To: Slaughter, Rebecca
Cc: Kopec, Janice
Subject: FW: Letter to the FTC Commissioners on Civil Rights and Privacy
Attachments: Letter to the FTC - Civil Rights and Privacy.pdf

Letter from more civil society groups asking for a rulemaking. (b)(5)
Many of these folks will be presenting tomorrow at the meeting with Sam and Erie.

From: Howard, Jennifer <jhoward1@ftc.gov>
Sent: Thursday, July 29, 2021 11:41 AM
To: Sara Collins (b)(6)@publicknowledge.org
Cc: Meyer, Erie K <emeyer@ftc.gov>; Laroia, Gaurav <glaroia@ftc.gov>; Spector, Robin <rspector@ftc.gov>; David Brody (b)(6)@lawyerscommittee.org; Dahdouh, Thomas N. <TDAHDOUH@ftc.gov>
Subject: Re: Letter to the FTC Commissioners on Civil Rights and Privacy

Hi Sara-

Thanks so much for sending. Look forward to discussing further and will be in touch!

Jen Howard
Chief of Staff
Federal Trade Commission
E: jhoward1@ftc.gov
O: [202-326-2408](tel:202-326-2408)

On Jul 29, 2021, at 11:38 AM, Sara Collins (b)(6)@publicknowledge.org wrote:

Hello,

Please find attached a letter to the Commissioners signed by twenty-five civil rights, consumer protection, and public advocacy organizations asking the FTC to address a variety of harms caused by big tech data practices. We are asking that the FTC (1) address any unfair and deceptive practices with all regulatory tools available, including rulemaking; (2) create an Office of Civil Rights; and (3) commit more resources to enforcing against civil rights and privacy UDAPs.

If you have any questions about the letter please email myself or David Brody.

Thank you for your time,

Sara Collins

--



Sara Collins

Policy Counsel

(b)(6) [@publicknowledge.org](mailto:(b)(6)@publicknowledge.org)

(b)(6)

Public Knowledge | [@publicknowledge](https://twitter.com/publicknowledge) | www.publicknowledge.org
1818 N St. NW, Suite 410 | Washington, DC 20036

<Letter to the FTC - Civil Rights and Privacy.pdf>

Chair Lina Khan
Commissioner Rohit Chopra
Commissioner Rebecca Slaughter
Commissioner Noah Phillips
Commissioner Christine Wilson

Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Chair Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson:

We, the undersigned civil rights, civil liberties, and consumer protection organizations, write to bring your attention to the urgent need for the Federal Trade Commission to protect civil rights and privacy in data-driven commerce. The Internet is an irreplaceable venue for free expression, trade, employment and housing opportunities, banking, education, entertainment, and, of course, civic engagement. As courts have recognized for decades and recently reaffirmed, privacy rights are civil rights¹ and commercial data practices are inextricably intertwined with equal opportunity.²

We ask the FTC to (1) initiate rulemaking and take other appropriate actions to regulate unfair and deceptive commercial data practices such as those discussed below; (2) create an Office of Civil Rights; and (3) commit greater resources to aggressively enforce against unfair and deceptive practices. We urge the FTC to use all tools at its disposal.

Unfair and Deceptive Commercial Data Practices Cause Substantial Harm

As has been extensively documented by independent researchers, journalists, courts, companies, and this Commission, unfettered data practices employed single-mindedly for private gain cause significant harm to the public. Tech companies directly cause or contribute to many of these harms. Like the sprawling consequences of historic redlining, other harms arise as negative externalities (including downstream effects) from data-exploitative business models and the market incentives they create. Addressing direct harms and changing incentives will have positive effects for the Internet ecosystem as a whole.

¹ See *Am. for Prosperity Found. v. Bonta*, ___ S.Ct. ___, 2021 WL 2690268, *6 (July 1, 2021) (discussing *NAACP v. Alabama*, 357 U.S. 449 (1958)).

² See *Leaders of a Beautiful Struggle v. Baltimore Police Dept.*, ___ F.4th ___, 2021 WL 2584408, *14 (4th Cir. June 24, 2021) (en banc) (Gregory, C.J., concurring) (discussing how past redlining of Baltimore continues to affect resource distribution and public well-being, including “investment in construction; urban blight; real estate sales; household loans; small business lending; public school quality; access to transportation; access to banking; access to fresh food; life expectancy; asthma rates; lead paint exposure rates; diabetes rates; heart disease rates” and more.).

Harms to Civil Rights and Equal Opportunity

- 1) Automated decision-making systems produce and reproduce new and longstanding patterns of discrimination in recruiting, employment, finance, credit, housing, K-12 and higher education, policing, probation, healthcare, as well as the promotion of key services through digital advertising.
 - a. Ex.: Facebook has been sued by advocates and the U.S. government for enabling discrimination by allowing advertisers to restrict ad viewership by race, religion, national origin, and other protected characteristics. Google and Twitter have similarly been investigated by HUD for housing discrimination.
- 2) Unscrupulous political operatives and foreign adversaries have used conventional advertising and targeting tools on social media platforms to interfere with U.S. elections and engage in voter suppression. Social media plays a key role in disinformation campaigns that spread conspiracy theories, threaten election integrity, and lead to violence such as the January 6 attack on the U.S. Capitol.
- 3) Disinformation campaigns in non-English languages are particularly rampant due to disregard by major platforms such as Facebook. The ability to target these types of campaigns depends on the privacy-invasive architecture of social media platforms.
- 4) Platform design choices routinely enable discrimination within important consumer services and workplaces.
 - a. Ex: Airbnb enabled landlords to reject prospective guests with what were perceived to be distinctly Black names at higher rates than guests with what were perceived to be distinctly white names.
 - b. Ex: Uber enabled drivers to discriminate against passengers with what were perceived to be distinctly Black names and provide more expensive services to women passengers. Uber likewise used biased consumer-reviews to make workplace decisions that may violate civil rights.
- 5) Social media firms' algorithmic design choices create pathways to white supremacy, which can lead to violence and deprivation of civil rights.
 - a. Ex: An internal Facebook study obtained by the Wall Street Journal noted that "64% of extremist group joins are due to our recommendation tools...our recommendation systems grow the problem."
 - b. Ex: YouTube video recommendations systemically recommend harmful and progressively more extreme content to viewers, creating pathways to radicalization.
- 6) Firms reify and advance existing social prejudices, particularly racism, throughout technology and online services, including through search engine and other predictive

text results, voice technologies, facial analysis, and other biometric and visual processing techniques.

- 7) Workers are increasingly monitored through digital surveillance programs in and beyond the place of employment, raising novel questions as to whether and how these applications enable exploitation and discrimination. Tech firms dehumanize workers through intrusive surveillance and intermediating working relationships with opaque, sometimes degrading workplace management software.
- 8) Delivery service drivers protested a nearly-invisible method of pay calculation that put customers' tips toward guaranteed minimum wages.
- 9) Platform companies use "psychological tricks" on workers, not dissimilar to the dark patterns used on consumers, to maximize company growth.
- 10) Facial recognition and other biometric surveillance technologies erode civil liberties, particularly for Black and Brown communities. The biases in these technologies and their use by law enforcement have led to traumatic violations of civil liberties, including a number of recent wrongful arrests of innocent Americans misidentified by faulty facial recognition software.
- 11) Ambient state and private surveillance in public spaces has a chilling effect on basic freedoms and disproportionately affects Black and Brown communities.

Harms to Consumer Protection and Invasions of Privacy

- 1) Digital firms employ "dark pattern" techniques to confuse and exploit consumers, including intentionally complicating the process of opting-out of data collections.
- 2) Digital firms use similar designs to trick consumers into sharing personal data or buying services they may not want.
- 3) Digital firms use similar designs to obscure pricing and fee structures for services up front.
- 4) Digital firms use similar designs and practices to make it difficult for consumers to change privacy settings, delete accounts, or cancel services.
- 5) Amazon has labeled as "Amazon's Choice" or sold from its warehouses products that are deceptively labeled, or have been declared unsafe or banned by federal regulators.
- 6) E-commerce sites like Amazon and Google have continued to sell items they promised to ban, such as pill presses that have been used to manufacture counterfeit prescription drugs or firearm accessories.
- 7) Millions of businesses listings on mapping sites are fraudulent with analysts cited by the WSJ estimating up to 11 million listings on Google maps may be false listings.

- 8) Negligence and lax safety standards enable bad actors to commit elaborate frauds on digital platforms.
 - a. Ex: Various Airbnb scams.
 - b. Ex: Applications on smartphone app stores with billions of downloads have been found to be committing ad fraud.
- 9) Research conducted by Consumer Reports found that nearly half of consumers struggle to distinguish between a paid ad and an objective search result.
- 10) Large online advertising platforms are combining data with real-world purchasing and customer information to track them across the web and in the physical world.
- 11) Navigation applications optimize routes for speed regardless of the negative impact on public safety and traffic. Multiple people have been killed by so-called “self-driving” or auto-pilot enabled cars on public roads. Some evidence suggests the entry of a ride-sharing application into a city increases the number of fatal accidents by 3%.
- 12) Platform transportation companies erode the hard-won public safety protections put in place over decades around seatbelts, child safety seats, distracted driving, helmet-wearing, and more.
- 13) E-commerce and platform companies whose delivery drivers kill or maim pedestrians refuse to take responsibility for those injuries, despite incentivizing dangerous driving behavior.
 - a. Ex: Amazon incentivized drivers to rush through holiday delivery. Upon being sued by the family of a pedestrian who was killed, they claimed: “The damages, if any, were caused, in whole or in part, by third parties not under the direction or control of Amazon.com.”
- 14) Firms’ amplification and enabling of public health misinformation at scale has eroded public trust in vaccines and public health officials. Too many American families and their loved ones have been severely harmed by their belief in misinformation, particularly during the COVID-19 pandemic, and vaccine hesitancy remains an issue.
- 15) Large online advertising platforms like Google have placed ads on sites promoting COVID-19 conspiracy theories in contrast to the commitments they made to combat COVID-19 misinformation.
- 16) Platform design choices that algorithmically amplify false information and propaganda in order to increase engagement on social media can grossly warp public discourse and understanding around public events, complicating the media landscape for consumers.

- 17) Firms track Americans in gross detail, relying on contrived interpretations of consumer consent or without explicit consent.
 - a. Ex. Mobile phone trackers collect precise location over 14,000 times per day.
- 18) Firms collect consumer data that they do not need without consent.
- 19) Firms accept and purchase user data collected by other firms without their consent.
 - a. Ex: Facebook received ovulation data from a third party without user consent.
- 20) Firms collect consumer data under the pretense of consent, perpetuating the fallacy that consumers are in a position to read, understand, or give informed consent (often consumers *must* use services and lack other options or the ability not to consent).
- 21) Firms use deceptive disclosures and settings to trick consumers into allowing data sharing with third parties.
- 22) Firms use personal consumer data—including private emails, conversations, and photographs—to develop algorithmic products without full consumer knowledge, consent, or reciprocity.
- 23) Firms fail to secure or delete obsolete user data, resulting in significant individual and collective costs. While firms may prefer to paint themselves as victims, a more apt metaphor might be oil companies who fail to prevent oil spills.
 - a. Ex: Experian’s API weakness likely exposed “most Americans” credit scores, creating a feeding frenzy for identity thieves.
 - b. Ex: Popular genetic testing services have insufficient security leading to significant potential for exploitation of genomic and health information.
- 24) Poor data protection can result in both exploitative and exclusionary conduct.
- 25) Privacy harms are especially acute in combination with competitive harms: experts have shown that firms that achieve market dominance and successfully suppress competitive threats are able to lower privacy protections to pursue and extract greater data gains from consumers.
 - a. Ex: Facebook pivoted away from privacy-protection toward privacy exploitation upon achieving significant market power.
- 26) Digital firms use unprecedented data collection and targeting tools to exploit behavioral shortcomings and biases amongst consumers in real-time.
- 27) Digital firms employ a bevy of dynamic pricing strategies, which nearly three-quarters of Americans think is a problem.

FTC Should Regulate and Stop Unfair and Deceptive Commercial Data Practices

The following practices relating to the use of consumers' personal data are unfair or deceptive. They cause many of the harms discussed above, either directly or by causing downstream negative externalities. The FTC should take immediate action to address them using all tools at its disposal, including but not limited to rulemaking.

Civil Rights and Equal Opportunity

- 1) Using criteria that have the purpose or effect of resulting in adverse eligibility determinations or to target or deliver advertisements for housing, employment, credit, insurance, or educational opportunities on the basis of protected characteristics. This does not include using protected characteristics (a) for legitimate self-testing for the purpose of preventing unlawful discrimination, complying with legal requirements, or assessing diversity, equity, and inclusion programs; or (b) for the bona fide and primary purpose of expanding an applicant, candidate, participant, or customer pool by increasing diversity and inclusion.
- 2) Using personal data to violate rights protected by federal law, where such rights are capable of being violated by a private actor. This includes using personal data to deprive or defraud someone of the right to vote in violation of federal law.
- 3) Disclosing non-public information related to an individual's sexual life without specific opt-in consent, such as their sexual activity, relationships, orientation, gender identity or expression, preferences, communications, or behavior. This does not include automated linking to, republishing of, or indexing such information if it was already disclosed by others—such as routine search engine operations.
- 4) Offering online services that are not accessible to persons with disabilities.
- 5) Failing to provide disclosures and policies in all languages in which the company routinely provides service.
- 6) Using machine learning or artificial intelligence technology to process personal data or aggregate data about a population without ensuring, prior to deployment and through regular assessment, that such processing does not directly or indirectly result in adverse eligibility decisions or exclusion from commercial opportunities on the basis of protected characteristics.
- 7) Using machine learning or artificial intelligence technology in a manner that does not comport with what the technology is marketed or represented to do, if such use causes harm to consumers.
- 8) Claiming that a product using machine learning or artificial intelligence technology can predict future outcomes with a degree of certainty or accuracy, or predict human behavior at all, if the claimant does not possess reliable evidence that such technology has any such capability greater than a simple linear regression analysis or random chance.

- 9) Representing that a product using machine learning or artificial intelligence technology has a source, sponsorship, approval, certification, accessories, characteristics, components, uses, or benefits that it does not have, or that such product is of a certain standard, quality, grade, style, or model when it is not.
- 10) Designing, modifying, or manipulating a user interface of a service, directed at children under the age of 13, with the purpose or substantial effect of cultivating compulsive usage.
- 11) Using personal data to target or deliver personalized advertisements to children under the age of 13. This does not include contextual advertising.
- 12) Using personal data to conduct psychological experiments on users without opt-in consent and compliance with best practices for such research, if it is reasonably foreseeable that such experiments may result in harm physical or mental health.

Data Protection

- 1) Failing to minimize data collection and retention. Collected data should be limited to what is necessary to provide the service requested by the consumer; should not be used for secondary purposes; and should not be retained for longer than is necessary to satisfy the purpose for which it was collected. Secondary uses should not be allowed without additional and specific opt-in consent.
- 2) Using facial recognition technology on persons in traditional public forums or places of public accommodation without opt-in consent.
- 3) Collecting, sharing, or otherwise using an individual's biometric data, including but not limited to facial recognition technology, without specific opt-in consent and without a valid business necessity.
- 4) Disclosing, without authorization or in excess of authorization, the content of a communication to anyone who is not a party to the communication or who does not have authorization to access it, including both state actors and private parties.
- 5) Collecting sensor recordings of environmental data from a consumer device, in conjunction with personal data, without opt-in consent. This includes data collected by a microphone, camera, or other sensors capable of measuring chemicals, light, radiation, air pressure, speed, weight or mass, positional or physical orientation, magnetic fields, temperature, or sound. This does not include processing by an entity that did not directly collect the data.
- 6) Collecting personal data as a third party about users of an online service, where such data is not publicly available, without opt-in consent from affected individuals. This includes, for example, cursor movements and clicks, heat maps, in-app activity, location information, third party tracking beacons and cookies, and other third-party methods of tracking user activity.

Due Process

- 1) Requiring consumers to consent to pre-dispute binding arbitration clauses or class action waivers.
- 2) Requiring consumers to waive privacy or other rights to obtain service or requiring that consumers who do not waive their rights pay a higher fee. This does not include customer loyalty programs, such as grocery store discount cards.
- 3) Denying consumers the ability to access, correct, delete, or port their personal data in response to a reasonable request.
- 4) Failing to provide an effective and prompt appeal when requests to access, correct, delete, or port data are denied.
- 5) Using dark patterns and other misleading user interfaces to unfairly or deceptively induce consent or other adverse actions from a consumer.

Transparency

- 1) Failing to affirmatively disclose, in a clear and conspicuous manner, how a data processor collects, uses, shares, and retains personal data, including failing to explain a consumer's ability to control the use of their data.
- 2) Failing to affirmatively disclose when and how a company uses machine learning or other artificial intelligence technology to process personal data, when such processing affects commercial goods, services, or opportunities that a consumer may receive. This includes failure to disclose non-sensitive information from risk assessments.
- 3) Failing to conspicuously provide all relevant privacy policies and controls in one place, such as scattering privacy policies, updates, or controls across multiple parts of a website or app. This practice is particularly deceptive when a consumer's intent to change a privacy control in one area can be undermined by failure to change other controls in other areas, and such discrepancy is not conspicuous.
- 4) Refusing to tell a consumer to whom the company disclosed their personal data, or with whom the company contracts to share such data, in response to a reasonable request.
- 5) Failing to notify a consumer when the company discloses their personal data to a state actor unless the company is legally required not to disclose.
- 6) Misstating or mischaracterizing the subject matter, methods, frequency, or results of any of one's own internal or external assessments.

Security

- 1) Failing to secure personal data, to protect the integrity of personal data, or to prevent unauthorized access or processing of personal data.

- 2) Failing to promptly notify affected parties following a data breach.
- 3) Failing to comply with state data breach laws and regulations when such failure affects interstate commerce and is not inconsistent with federal law.
- 4) Disclosing non-public personal data to a service provider or third party without contractually requiring the service provider or third party to meet the same privacy standards as the company, or without engaging in reasonable oversight to ensure compliance with such requirements.

Accountability

- 1) Retaliating against whistleblowers who attempt to report unfair or deceptive practices.
- 2) Knowingly aiding and abetting another person engaging in an unfair or deceptive practice.
- 3) Failing to report to the Commission if a company has knowledge that a service provider, affiliate, or customer has engaged in an unfair or deceptive practice involving the company's goods or services. This does not include content immunized by 47 U.S.C. 230.
- 4) Failing to provide an annual sworn certification from a C-suite officer or equivalent senior officer that a company (other than a small business) is fully compliant with the FTC's data privacy rules.

Office of Civil Rights

The FTC should create an Office of Civil Rights. There are more than 30 civil rights offices within federal agencies. The harms and unfair or deceptive practices discussed in this letter are part of a large, interconnected data ecosystem. Expanding the Commission's expertise on discrimination and equal opportunity will help it holistically assess the equities of modern digital trade. Such an Office will create a focal point for Agency expertise and stakeholder engagement on these important issues. The Office could also advise on actions the Commission may take, and coordinate with other agencies, to help respond to commercial data practices that may result in unjust disparate treatment or impact on the basis of race, ethnicity, religion, national origin, immigration status, disability, sex, gender identity or expression, sexual orientation, age, or familial status.

As the FTC looks to chart a new course for oversight of unfair and deceptive practices arising from commercial data practices and big tech, we look forward to working with you to protect civil rights, promote algorithmic fairness, advance equal opportunity, and preserve privacy and free expression.

For more information, please contact David Brody and Sara Collins.

Sincerely,

Access Now

Accountable Tech

Asian Americans Advancing Justice | AAJC

American Association for Justice

ADL

Center for American Progress

Center for Digital Democracy

Center for Democracy and Technology

Center of Privacy & Technology at Georgetown Law

Common Sense Media

Consumer Action

Consumer Federation of America

Electronic Privacy Information Center

HTTP

Lawyers' Committee for Civil Rights Under the Law

Media Alliance

National Council of Asian Pacific Americans

National Fair Housing Alliance

National LGBT Task Force

OCA – Asian Pacific American Advocates

Public Citizen

Public Knowledge

Ranking Digital Rights

The Greenlining Institute

From: Kopec, Janice
Sent: Wed, 12 May 2021 03:17:11 +0000
To: Holland, Caroline; Mark, Synda; Slaughter, Rebecca
Subject: (b)(5)
Attachments:

(b)(5)

From: Josh Golin
Sent: Thu, 25 Jul 2019 15:04:24 -0400
To: Simons, Joseph; Phillips, Noah; Wilson, Christine; Slaughter, Rebecca; Chopra, Rohit
Cc: Crawford, Molly; Magee, Peder; Laura Moy; Angela Campbell; Lindsey Barrett; David Monahan; Jeffrey Chester
Subject: Important new research on YouTube's popularity with children
Attachments: Pew YouTube Report 2019.pdf

Dear Chairman Simons, Commissioner Phillips, Commissioner Chopra, Commissioner Slaughter, and Commissioner Wilson,

In case you missed it, Pew released an important new study today that examined the most popular channels on YouTube. As far as I know, it's the first study that uses human coders to determine if YouTube videos are "child-directed." The study examined one-week of videos from the 43,770 channels with at least 250,000 subscribers: Among the key findings:

Videos aimed at children were highly popular, as were those that featured children under the age of 13 – regardless of their intended audience. Only a small share of English-language videos posted by these popular channels during the study period were explicitly intended for children (based on a consensus of human coders). But those that tended to be longer received more views, and came from channels with a larger number of subscribers relative to general-audience videos. More broadly, videos featuring a child or children who appeared to be under the age of 13 – regardless of whether the video in question was aimed exclusively at children or not – received nearly three times as many views on average as other types of videos. And the very small subset of videos that were directly aimed at a young audience and *also* featured a child under the age of 13 were more popular than any other type of content identified in this analysis as measured by view counts.

And:

Children's videos tended to be longer and received more views than many other types of content; a large share of these videos focused on toys or games

In total, just 4% of all English-language videos posted by popular YouTube channels in the first week of 2019 appeared to be aimed at children under the age of 13. But despite comprising a relatively small share of the total, children's videos tended to be longer, received more views, and came from channels with a greater number of subscribers relative to content aimed at a general (teen or adult) audience. Videos that appeared to be intended for children averaged 153,227 views (median of 17,540), compared with an average of 99,713 views (14,187 median) for other videos. Channels that posted children's videos also had many more subscribers: 1.9 million on average (872,188 median) vs. 1.2 million (586,588 median) among channels that did not post a video aimed at children during the week. And half of all children's videos lasted at least 11 minutes, compared with a median of 7 for other videos.

As noted above, children's content could belong to any of the other topical categories in this analysis, and children's content related to toys or games (excluding video games) was both highly common and tended to receive many views. Some 28% of children's videos were related to toys or games, and these videos received an average of 147,923 views (30,929 median), compared with 109,585 views (22,871 median) for toys or games videos aimed at a general audience.

Channels that produced videos about toys or games – especially those that appeared to target children – also had more subscribers than average. Channels that produced at least one video

during this week about toys or games that was aimed at children had, on average, 2.1 million subscribers (median of 1.1 million), compared with 1.2 million (586,126 median) for channels that did not produce any videos meeting this description.

We believe these findings are significant because they demonstrate, with rigorous methodology, that portions of YouTube are clearly child-directed and have large child audiences. We also note how much of the popular children's content is designed to promote toys and other products, an issue we've raised at the Commission on a number of occasions.

I've attached the study and here is the [LA Times reporting](#) on the research.

We continue to hope that the Commission's final settlement with Google will include significant measures to ensure that YouTube is COPPA compliant going forward as we outlined in our letter of June 25th and subsequent phone conversations. Please don't hesitate to contact me if you have questions.

Thank you for your time and attention to this critical matter,

Josh

Josh Golin

Executive Director

CCFC: Campaign for a Commercial-Free Childhood

(b)(6)

<http://www.commercialfreechildhood.org>

Stand up for children: [Support CCFC](#)

FOR RELEASE JUL. 25, 2019

A Week in the Life of Popular YouTube Channels

An analysis of every video posted by high-subscriber channels in the first week of 2019 finds that children’s content – as well as content featuring children – received more views than other videos

BY *Patrick Van Kessel, Skye Toor and Aaron Smith*

FOR MEDIA OR OTHER INQUIRIES:

Patrick van Kessel, Senior Data Scientist
Shawnee Cohn, Communications Manager

202.419.4372
www.pewresearch.org

RECOMMENDED CITATION

Pew Research Center, July 2019, “A Week in the Life of Popular YouTube Channels”

About Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. The Center conducts public opinion polling, demographic research, content analysis and other data-driven social science research. It studies U.S. politics and policy; journalism and media; internet, science and technology; religion and public life; Hispanic trends; global attitudes and trends; and U.S. social and demographic trends. All of the Center's reports are available at www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts, its primary funder.

© Pew Research Center 2019

A Week in the Life of Popular YouTube Channels


An analysis of every video posted by high-subscriber channels in the first week of 2019 finds that children’s content – as well as content featuring children – received more views than other videos


The media landscape was upended more than a decade ago when the video-sharing site YouTube was launched. The volume and variety of content posted on the site is staggering. The site’s popularity makes it a launchpad for performers, businesses and commentators on every conceivable subject. And like many platforms in the modern digital ecosystem, YouTube has in recent years become a flashpoint in ongoing debates over issues such as [online harassment](#), [misinformation](#) and the impact of technology on [children](#).


Amid this growing focus, and in an effort to continue demystifying the content of this popular source of information, Pew Research Center used its own custom [mapping technique](#) to assemble a list of popular YouTube channels (those with at least 250,000 subscribers) that existed as of late 2018, then conducted a large-scale analysis of the videos those channels produced in the first week of 2019. The Center identified a total of 43,770 of these high-subscriber channels using a process similar to the one used in our [study of the YouTube recommendation algorithm](#). This data collection produced a variety of insights into the nature of content on the platform:

The YouTube ecosystem produces a vast quantity of content. These popular channels alone posted nearly a quarter-million videos in the first seven days of 2019, totaling 48,486 hours of content. To put this figure in context, a single person watching videos for eight hours a day (with no breaks or days off) would need more than 16 years to watch all the content posted by just the most popular channels on the platform during a single week. The average video posted by these channels during this time period was roughly 12 minutes long and received 58,358 views during its first week on the site.

A week in the life of popular YouTube channels


 **43,770** channels with at least **250,000** subscribers

 **56%** posted a video during the first week of 2019

 **243,254** videos

 Just **17%** were in English

 Over **48,000** total hours

 Over **14 billion** views in one week

Source: Analysis of videos posted Jan. 1-7, 2019, by YouTube channels with at least 250,000 subscribers, collected using the YouTube Data API.

“A Week in the Life of Popular YouTube Channels”

PEW RESEARCH CENTER

Altogether, these videos were viewed over 14.2 billion times in their first seven days on the platform.¹

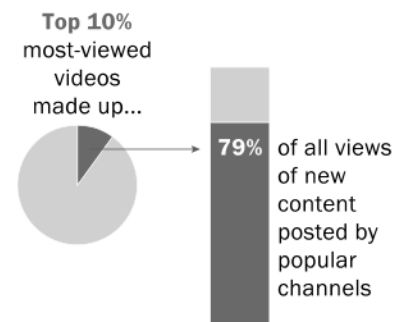
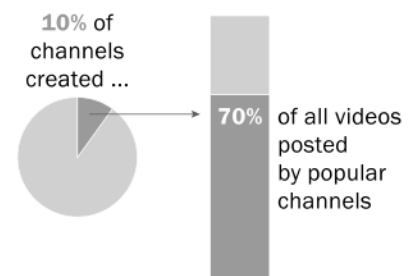
YouTube is a global phenomenon, and its most popular channels posted a substantial amount of content in languages other than English. Using a combination of hand-labeling and machine learning, the Center categorized videos based on whether or not they contained any text or audio in a language other than English. The results of this analysis illustrate the global nature of the YouTube platform. Just over half of these channels (56%) posted a video during the first week of 2019, and the majority of these active channels (72%) posted at least one video that was partially or completely in a language other than English. Overall, just 17% of the nearly quarter-million videos included in this analysis were fully in English.

A small share of highly active creators produced a majority of the content posted by these popular channels. As is the case with many online platforms (such as [Twitter](#)) a relatively small share of channels were responsible for a majority of the content posted during the study period. Just 10% of the popular channels identified in the Center’s mapping produced 70% of all the videos posted by these channels during the first week of 2019. Similarly, the 10% of popular-channel videos that had the most views in this period were responsible for 79% of all the views that went to new content posted by these channels.

The total number of high-subscriber channels increased dramatically in the second half of 2018. The Center’s mapping process identified 9,689 channels that crossed the 250,000-subscriber threshold between July 2018, when the Center last conducted [an analysis of YouTube data](#), and December 2018, when the data was updated for this analysis. That represents a 32% increase in the total number of popular channels over that period. By the same token, the number of

Large majority of videos from popular YouTube channels came from a small share of producers

Of YouTube videos produced by popular channels during the first week of 2019 ...



Source: Analysis of videos posted Jan. 1-7, 2019, by YouTube channels with at least 250,000 subscribers, collected using the YouTube Data API.

"A Week in the Life of Popular YouTube Channels"

PEW RESEARCH CENTER

¹YouTube uses a proprietary algorithm to determine how many times a video has been watched by actual humans, as opposed to computer programs. While it has not released an official threshold, a [number of third parties](#) report that "views" do not appear to be counted unless a user watches at least 30 seconds of a video.

subscribers to existing popular channels that had already been identified as of July 2018 increased by an average of 27% over the same period.

In addition to this broader data collection, Pew Research Center also conducted a separate content analysis of the English-language videos posted by these popular channels over the first week of 2019 (in total, 37,079 videos met this description). The Center used human coders to identify the primary category or theme of each video (such as video games, consumer technology or current events and politics), and also examined the keywords used in video titles and descriptions to identify words that were widely used and associated with higher view counts relative to other videos. Some of the key findings from this analysis include:

Videos aimed at children were highly popular, as were those that featured children under the age of 13 – regardless of their intended audience. Only a small share of English-language videos posted by these popular channels during the study period were explicitly intended for children (based on a consensus of human coders). But those that were tended to be longer, received more views, and came from channels with a larger number of subscribers relative to general-audience videos. More broadly, videos featuring a child or children who appeared to be under the age of 13 – regardless of whether the video in question was aimed exclusively at children or not – received nearly three times as many views on average as other types of videos. And the very small subset of videos that were directly aimed at a young audience and *also* featured a child under the age of 13 were more popular than any other type of content identified in this analysis as measured by view counts.

It should be noted that YouTube explicitly states that the platform is not intended for children under the age of 13. YouTube provides a [YouTube Kids](#) platform with enhanced parental controls and curated video playlists, but the analysis in this report focuses on YouTube as a whole.

English-language videos related to current events or politics posted by these popular channels tended to have an international (rather than U.S.) focus. Videos explicitly related to current events or politics were relatively common, comprising 16% of all English-language videos uploaded during the study period. However, the majority of these videos were international in focus and did not mention events, issues or opinions related to the United States. While channels that posted one or more U.S. current events or politics videos were particularly active – posting an average of 63 total videos during the week – U.S. current events or politics videos comprised just 4% of all of the videos that were posted by popular channels overall.

