Arizona Law Journal of Emerging Technologies

Volume 7 *Article 7*

5-2024

EMPOWERING EVERYDAY AMERICANS: THE ALGORITHMIC CHOICE AND TRANSPARENCY ACT (THE "ACT ACT")

Brian K. Keller

2023-2024 https://azlawjet.com Vol. 7, Art. 7

Arizona Law Journal of Emerging Technologies

EMPOWERING EVERYDAY AMERICANS: THE ALGORITHMIC CHOICE AND TRANSPARENCY ACT (THE "ACT ACT")

Brian K. Keller

Table of Contents

EMPOWERING EVERYDAY AMERICANS: THE ALGORITHMIC CHOICE AND TRANSPARENCY ACT (THE "ACT ACT")

Brian K. Keller[*]

I. Introduction

An estimated $221 billion was spent on digital ads in the United States in 2022.[1] Internet companies like Facebook,[2] Twitter, Instagram, YouTube,[3] Google[4] and Bing search, and TikTok,[5] vacuum up personal data from Americans, then charge third parties to use that personal data to target Americans with ads or offer them subscription services. Addictive-behavior-forming algorithms on social media sites, and on internet search engines, along with "walled digital gardens" and lack of data portability, keep users coming back to these sites to serve them targeted and personalized content.[6] Social media and search engines are massive, complex, commercial advertisement engines that masquerade as free search, email, and social media for their unsuspecting users.

Americans have little control, and little clarity, over how Twitter, Facebook, TikTok, YouTube, Instagram, Twitch, and others, serve-up content to their phones, Smart TVs, PCs, tablets, watches, game consoles, and more. An Amnesty International study concluded that Facebook amplified, promoted, and recommended content inciting violence, hate, and discrimination against the Rohingya Muslims in Myanmar, playing a part in their murder and ethnic cleansing by Myanmar's

[*] Brian Keller is an appellate litigator, served as a Marine Corps officer and judge advocate, and recently completed a Masters of Law in National Security and Cybersecurity Law. The views presented here are his own and do not necessarily represent the views of the U.S. Department of Defense, its Components, or any other arm of the U.S. Government.

[1] *Digital Advertising Spending in the United States in 2022, by Industry,* STATISTA (Aug. 29, 2023), https://www.statista.com/statistics/301876/distribution-digital-ad-spend-by-industry-channel-usa/.

[2] Len Sherman, *Why Facebook Will Never Change Its Business Model,* FORBES (Apr. 16, 2018, 1:01 PM), https://www.forbes.com/sites/lensherman/2018/04/16/why-facebook-will-never-change-its-business-model/.

[3] Nick Statt, *YouTube is a $15 Billion-a-year Business, Google Reveals for the First Time,* THE VERGE (Feb. 3, 2020, 2:24 PM), https://www.theverge.com/2020/2/3/21121207/youtube-google-alphabet-earnings-revenue-first-time-reveal-q4-2019.

[4] Megan Graham & Jennifer Elias, *How Google's $150 Billion Advertising Business Works,* CNBC (Oct. 13, 2021, 12:52 PM), https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html.

[5] Zheping Huang, *TikTok Has a Few Main Ingredients for Making Money,* BLOOMBERG (June 28, 2022, 6:45 AM), https://www.bloomberg.com/news/newsletters/2022-06-28/how-does-tiktok-make-money-app-relies-on-a-few-main-ingredients.

[6] *Id*.

security forces—and Facebook itself conceded that it could have done more to stop the viral anti-Rohingya hate speech and fake news from flooding Facebook's algorithmic social media feeds.[7]

Search, trending, and recommendation algorithms played a part in almost 150 million users on Facebook alone[8] engaging with anti-Hillary Clinton content and pro-Trump content in the 2016 American elections, part of what the Mueller Report called Russia's "sweeping and systemic" interference in the 2016 presidential elections.[9] As Anne Applebaum and Peter Pomerantsev put it, "[t]he buttons we press and the statements we make online are turned into data, which are then fed back into algorithms that can be used to profile and target us . . ."[10]

Two key problems afflict everyone in America—and for ten years, they have haunted our daily lives, and the daily news. First, Americans have no choice in whether algorithms are applied to their search engines and social media feeds. Nothing requires internet services or applications to allow consumers to easily "turn off" these algorithms that are used to profile and target us. And second, Americans don't understand how these algorithms affect the lives they live increasingly online. Researcher access to social media company data has helped shed light on how these algorithms work—but the companies routinely limit or terminate access to the type of data that could help explain the effects of algorithms on society. Not only that: but the companies that use these algorithms to maximize their profit both decline to disclose information about their algorithms citing "trade secrets," and often the companies cite a "black box problem"—that is, not even their computer programmers can explain exactly why the algorithms radicalize Americans, drive some to commit suicide, or cause any of the other harms that are so obviously caused by the mechanisms of our online world.

But some want to do nothing to change the status quo. They think this unchecked manipulation of and denial of choice to the American public, and keeping these algorithms and their machinations under the lock and key of social media companies and big tech businesses, is "good enough" for Americans. In spring 2023, Elon Musk's Twitter decided to lift a prior ban and enable Twitter to again algorithmically promote Kremlin-, China-, and Iran-controlled state media to its over 350 million users—including millions of Americans.[11] The Atlantic Council's Digital Forensic Research Lab summed it up: "Twitter users no longer must actively seek out state-sponsored content in order to see it on the platform; it can just be served to them," that is, "amplified" by

[7] *See Myanmar: The Social Atrocity: Meta and the Right to Remedy for the Rohingya,* AMNESTY INT'L (Sep. 29. 2022), https://www.amnesty.org/en/documents/ASA16/5933/2022/en/; Paul Mozur, *A Genocide Incited on Facebook, With Posts from Myanmar's Military,* N.Y. TIMES (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html; Karen Hao, *How Facebook got addicted to spreading misinformation,* MIT TECH. REV. (Mar. 11, 2021), https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/.

[8] Renee DiResta, *Computational Propaganda: Public relations in a high-tech age,* THE YALE REV. (Oct. 1, 2018), https://yalereview.org/article/computational-propaganda.

[9] SPECIAL COUNSEL ROBERT S. MUELLER, III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 ELECTION, Vol. I, 1-5 (2019).

[10] Anne Applebaum & Peter Pomerantsev, *How to Put Out Democracy's Dumpster Fire,* THE ATLANTIC, (Mar. 11, 2021, 8:41 AM), https://www.theatlantic.com/magazine/archive/2021/04/the-internet-doesnt-have-to-be-awful/618079/.

[11] David Klepper, *Twitter Changes Stoke Russian, Chinese Disinformation,* PBS NEWSHOUR (Apr. 24, 2023, 6:58 PM), https://www.pbs.org/newshour/politics/twitter-changes-stoke-russian-chinese-disinformation.

Twitter's algorithm, "as a way to help [the accounts] reach bigger audiences."[12] And while Facebook has temporarily adjusted its algorithms from time to time in response to elections and other events to dial-back the feeding of extreme content to users, the site invariably turns the algorithms back on.[13]

We have waited long enough. Things need to change.

II. Internet Recommendation Algorithms: American Ingenuity and Invisible Enemy

a. Big tech search- and social media algorithms pose dilemmas for free speech, technology, notice, consent, and national security.

Most Americans know there's a problem: some on the right think social media company algorithms suppress conservative speech and elevate speech from the left; some on the left think that social media companies amplify conspiracy theorists and white supremacists; and everybody seems to agree that algorithms serve up addictive junk harmful to our children, and to us. But despite knowing that we have a problem, we keep running into brick walls and each other, unable to find a solution.

But we cannot wait. The problem is dividing us, and there are simple solutions that we must enact now. Everyday Americans need to be empowered. They need to get to work educating themselves and building consensus. And Americans need to be provided the tools to do so free of the filter bubbles, the viral algorithms tending towards extreme content. They need to be free to choose, once well informed about how these ingenious algorithms shape our daily lives. That is, there are common sense, simple solutions to these problems that we've enacted many times before. We just need to remember our history.

i. The First Amendment narrows how Congress can solve the virality problem.

"Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble . . ."[14] The First Amendment to the United States Constitution is every American's birthright; it constrains the government's ability to make laws restricting speech based on content.[15] "[A]s a general matter, the First Amendment means that the government has no power to restrict expression because of its . . . content."[16] Regulation of speech by the government is not impossible, but the Supreme Court is undecided on the legal test to apply to prohibitions on false speech.[17] The more stringent test, strict scrutiny, applies when speech

[12] *Id.*
[13] *See infra* p. 9.
[14] U.S. CONST. amend. I.
[15] *Austin v. Reagan Nat'l Adver. of Austin, LLC*, 142 S. Ct. 1464, 1472 (1922).
[16] *United States v. Alvarez,* 567 U.S. 709, 716 (2012).
[17] *See United States v. Perez*, 43 F.4th 437, 444 n.3 (5th Cir. 2022) (*citing United States v. Alvarez*, 567 U.S. 709, 724 (2012) (plurality opinion) (applying strict scrutiny), and *id*. at 730-31 (Breyer, J., concurring in the judgment) (applying intermediate scrutiny)).

restrictions are content based, holding that such laws are presumptively unconstitutional unless the government shows the law is narrowly tailored—the least restrictive means of targeting speech[18]—and that the law serves a compelling government interest.[19]

A less stringent standard, intermediate scrutiny, applies when speech restrictions are content-neutral, and the government must show that such a speech restriction is "narrowly tailored to serve a significant government interest, and leave open ample alternative channels of communication."[20]

But any attempt by the federal government to forbid the posting of misinformation or disinformation online would presumptively fail. The Supreme Court in 2023 upheld, on First Amendment grounds, the right of website designers to refuse to make a website for homosexual weddings, where the designer believed that homosexuality "contradicts biblical truth"; the Court reasoned that the First Amendment protects the "freedom to think as you will and to speak as you think."[21] And the Court upheld the right of protestors to picket the funeral of American servicemembers and spread vile messages demeaning homosexuals.[22] The Court upheld the right of American Nazis to parade and "[d]istribut[e] pamphlets [and] display[] . . . materials which incite or promote hatred against persons of Jewish faith or ancestry."[23]

Not only does First Amendment precedent risk finding content-based restrictions on internet platforms presumptively unconstitutional, but the political climate would make it next to impossible to reach agreement on what domestic speech is misinformation or disinformation—and what speech is true. Indeed, the Supreme Court has been clear, in setting aside a conviction for lying about holding the Congressional Medal of Honor, that while content-based restrictions on speech are permitted for incitement, obscenity, defamation, speech linked to criminal conduct, "fighting words," child pornography, fraud, and grave and imminent threats—otherwise, the government cannot criminalize merely false speech.[24]

On the other hand, instead of regulating the content posted by the users of internet services like Facebook or TikTok or the site formerly known as "Twitter," one might instead regulate the *algorithms* used by commercial social media companies and search engine providers by requiring them to disclose to users how these algorithms work. One might require providing users the choice to display content from search results and social media feeds in a non-algorithmic manner.

This makes sense, given that not only false speech "goes viral"—so does true speech. False speech can be addressed in a number of ways, depending on whether it may be lawfully regulated, but the problem of virality is what to do about the *quick spread* of false speech where the quick spread *is* the harm. That is, the quick spread of harmful speech makes the speech no more false. And the content of the speech is not what makes the algorithm addictive. What we must regulate, then, is the algorithm itself.

[18] *United States v. Playboy Ent. Grp., Inc.,* 529 U.S. 803, 813 (2000).

[19] *Perry Educ. Ass'n v. Perry Loc. Educators' Ass'n,* 460 U.S. 37, 45 (1983).

[20] *Id.* at 45.

[21] *303 Creative LLC v. Elenis*, 143 S. Ct. 2298 (2023).

[22] *Snyder v. Phelps,* 562 U.S. 443 (2011).

[23] *Nat'l Socialist Party v. Skokie,* 432 U.S. 43 (1977).

[24] *United States v. Alvarez,* 567 U.S. 709 (2012).

This begs the question of whether, if we regulate only the algorithm, the recommendation algorithms themselves are speech at all, and whose speech is it. Since the algorithm is the proprietary computer code of the online platform, it is self-evidently the speech of that platform. Thus the recommendation algorithms might be the commercial speech of the online platforms, as some have argued[25] and some courts have recognized, that may be regulated—yet may also receive First Amendment protections as commercial speech, depending on whether are regulating based on content, or the regulation is content-neutral.[26] We examine this further below.

ii. Around 2010, America got addicted: In the 1990s Americans rarely used the internet; in 2023 we spend over two hours a day on social media alone.

One problem causing Congressional inaction on the algorithm problem is the vast social change wrought by social media in the short space of twenty-five years. The effects of this change on book-reading and traditional social structures, on policymaking and issues of constitutional law, are still being understood. Grappling with this history for those in the House and Senate is crucial—and understanding the history may enable the United States to catch up to groundbreaking legislation enacted by our European allies addressing this issue.

Before Facebook, the internet was largely like Wikipedia: we actively went out looking for the content we wanted in chat rooms, on bulletin boards, on our personal blogs, and with search engines. We collaborated to produce content and shared information about popular bulletin boards and blogs by word of mouth or email.[27] In 1996, Americans spent fewer than thirty minutes a month surfing the web; by 2009, Americans spent 27 hours a month online; by 2023, the average American spends over 60 hours a month *on social media alone*—not counting online games, web searches, and watching videos.[28]

Before 2005, only 12% of 18-29 year olds used social media; but by 2010, almost 80% of that same age group were on various social media platforms.[29] What were people doing online back then? In 2005, most people were using Yahoo, trailed by Google, MSN, and AOL: many of those platforms offered internet search functions paired with email and chat services; some also offered rudimentary links to news and external content.[30] By 2012, Google and its search engine shot to

[25] Kerri A. Thompson, *Commercial Clicks: Advertising Algorithms as Commercial Speech*, 21 VAND. J. ENT. & TECH. L. 1019, 1032 (2020), https://scholarship.law.vanderbilt.edu/jetlaw/vol21/iss4/4/.

[26] *See, e.g., Search King, Inc. v. Google Tech., Inc.,* No. CIV-02-1457-M, 2003 U.S. Dist. LEXIS 27193, *13 (W.D. Okla. May 27, 2003); *cf. Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001); *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132, 1141 (9th Cir. 1999).

[27] Applebaum & Pomerantsev, *supra* note 10 (describing Harvard Law professor's description of the "generative" internet that arrived with top-down, content-pushing sites like Facebook).

[28] Farhad Manjoo, *Jurassic Web,* SLATE (Feb. 24, 2009, 5:33 PM), https://slate.com/technology/2009/02/the-unrecognizable-internet-of-1996.html; Belle Wong, *Top Social Media Statistics and Trends of 2023,* FORBES ADVISOR (May 18, 2023, 2:09 PM), https://www.forbes.com/advisor/business/social-media-statistics/.

[29] Andrew Perrin, *Social Media Usage: 2005-2015,* PEW RESEARCH CENTER (Oct. 8, 2015), https://www.pewresearch.org/internet/2015/10/08/social-networking-usage-2005-2015/.

[30] *See* Carmen Ang, *Ranked: The Most Popular Websites Since 1993,* VISUAL CAPITALIST (Aug. 31, 2020) https://www.visualcapitalist.com/most-popular-websites-since-1993/; Paul R. La Monica, *The Internet Wars: A Report Card,* CNN (May 4, 2006, 3:19 PM) https://money.cnn.com/2006/05/04/technology/search_reportcard/index.htm.

the head of the pack, while Facebook and its algorithmic News Feed catapulted the service from obscurity in 2005 to the second most visited site, followed by YouTube, leaving Yahoo in fourth place.[31]

Following the development of Facebook's algorithmic "News Feed" post-2010, alongside similar top-down algorithms, the online tectonic plates had shifted: instead of facilitating users' chat and search activities online, internet services began *actively* pushing content before passive users' eyes, driven by Facebook's algorithms that determined what content users were likely to engage with—resulting in a parasitic relationship where internet content providers began to "game" Facebook's algorithms, increasingly supplying content that Facebook's algorithm would likely promote to users.[32] The internet services' focus on growth led to a "shadow industry of fake followers and artificial engagement," well known to the social media companies but not admitted publicly.[33] After around 2010, internet services, and users themselves, increasingly worked to make Americans "passive" recipients of content.[34]

iii. "Such messages spread like spores:" The virality problem.

This force-fed content experienced by the 72% of Americans using social media sites,[35] and the nearly 50% who "often" or "sometimes" rely on these platforms for news,[36] would not be a problem if the recommendation and search algorithms didn't fuel "virality"—that is, supercharged disinformation served to "everybody, everywhere, all at once."[37]

Social media recommendation algorithms, catering to vast American user platforms—like YouTube's almost 270 million, Facebook's almost 230 million, or Twitter's or TikTok's approximately 75 million American users[38]—are the secret sauce that make false, and sometimes harmful, social media content spread lies "like spores."[39] YouTube's internal research shows that adjusting recommendation algorithms can substantially alter user behavior, including a 70%

[31] Ang, *supra* note 30.

[32] Will Oremus et al., *How Facebook Shapes Your Feed*, WASH. POST (Oct. 26, 7:00 AM), https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works/.

[33] Joan Donovan, *How Social Media's Obsession with Scale Supercharged Disinformation*, HARVARD BUS. REV. (Jan. 13, 2021), https://hbr.org/2021/01/how-social-medias-obsession-with-scale-supercharged-disinformation.

[34] Applebaum & Pomerantsev, *supra* note 10.

[35] Brooke Auxier & Monica Anderson, *Social Media Use in 2021,* PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/.

[36] *Social Media and News Fact Sheet,* PEW RSCH. CTR. (Sep. 20, 2022), https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/.

[37] EVERYTHING, EVERYWHERE ALL AT ONCE (A24, 2022) (a popular film about the immigrant experience in America, family relationships, and saving the multiverse).

[38] *Social Media Fact Sheet,* PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media/?tabId=tab-4abfc543-4bd1-4b1f-bd4a-e7c67728ab76.

[39] Andrew Nikiforuk, *A Convoy Revved by Foreign Actors Spreading Lies,* THE TYEE (Feb. 21, 2022), https://thetyee.ca/Analysis/2022/02/21/Convoy-Revved-Foreign-Actors-Spreading-Lies/ (how Russian disinformation, injected into and gaming social media recommendation algorithms, undermined Canada's NATO mission in Latvia by spreading lies that Canadian troops were infecting locals with COVID, and generated artificial support for the Canadian trucker convoy).

reduction in viewing radicalizing content; but, YouTube declined to release the data needed for external validation.[40]

Facebook repeatedly confessed similar facts publicly. Prodded by Congressional hearings and bad press, Facebook made internal, but opaque, changes to recommendation algorithms during pivotal events such as the November 2020 elections and April 2021 Derek Chauvin trial, reducing the spread of algorithmic disinformation of algorithmically-driven extremist content; however, these modifications were situational and temporary.[41] Until the January 6th insurrection caused Facebook and Twitter to purge QAnon content, both sites facilitated the dissemination of QAnon content, with Facebook's recommendation algorithm actively promoting users to join QAnon groups, some of which gained hundreds of thousands of followers.[42]

A 2023 study published by Science demonstrates that disabling the standard personalized recommendation algorithm on Facebook and Instagram for ninety days, and showing users a purely chronological feed, did not counteract users' prior level of polarization.[43] But turning off the personalized recommendation algorithm had numerous benefits: (1) it increased the content users saw from "ideologically moderate friends"; (2) it increased diversity of sources beyond content the user already likely agreed with to a broad variety of information from "mixed audiences"; (3) it decreased the user's viewing of "uncivil" content; (4) decreased the user's viewing of content with "slur words"; (5) it decreased the amount of time the user spent on each site; and, (6) reduced the amount of content the users interacted with or shared by up to fifty percent.[44] Interestingly, those with chronological feeds increased the time spent on other sites with algorithmic feeds, including YouTube and TikTok[45]—the "addictive" pull and withdrawal effects of personalization algorithms could not be clearer.

The Science authors found that their results supported the rather obvious, and common belief, that algorithmic feeds "promot[e] an 'echo chamber' or 'filter bubble' effect."[46] It should not be surprising, then, that almost sixteen years into our worldwide experiment subjecting citizens to algorithm-enforced filter-bubbles, ninety days was insufficient to "depolarize" users' prior views.

And a 2021 survey of two years of reported algorithm-linked harms in Media and Communication, found that algorithms on social media (a) can be manipulated by users for commercial and abusive purposes, in ways that cause harm, (b) reinforce, strengthen, and amplify phenomena dangerous to democracy, including hate speech, disinformation, and radicalization, (c) promote addictive behavior and erode privacy of users, and (d) provide powerful internet companies, through the combination of the algorithm with big data, a "God view" creating an unequal relationship between

[40] Paul M. Barrett et al., *REPORT: Fueling the Fire: How Social Media Intensifies U.S. Political Polarization—And What Can Be Done About It,* NYU STERN CTR. FOR BUS. AND HUM. RTSS 11 (Sep. 12, 2021), https://bhr.stern.nyu.edu/blogs/2021/report-fueling-the-fire.

[41] *Id.* at 12-14; Jeff Horwitz & Deepa Seetharaman, *Facebook Executives Shut Down Efforts to Make the Site Less Divisive,* WALL ST. J. (May 26, 2020, 11:38 AM), https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

[42] Barrett, et al., *supra* note 40, at 13.

[43] Andrew M. Guess et al., *How Do Social Media Feed Algorithms Affect Attitudes and Behavior in an Election Campaign?,* 381 SCIENCE 398, 402 (July 27, 2023), https://www.science.org/doi/10.1126/science.abp9364.

[44] *Id.* at 398, 400-403.

[45] *Id.* at 400.

[46] *Id.* at 401.

the platforms, users, and markets.[47] The authors noted the "failures of social media companies in addressing algorithmic harm," and praised the European Commission's Digital Services Act—discussed *infra*[48]—which proposed requiring transparency in the use of algorithms, providing users an opportunity to opt-out of personalized algorithms, and auditing of how recommendation algorithms work.[49]

But it *is* encouraging that the simple act of removing the recommendation algorithm, in favor of a non-algorithmic chronological[50] listing of content, decreases the "filter bubble effect" that favors presenting extreme and uncivil content to users. Given that one-third of Facebook users consume news on the platform,[51] the increased amount of time reading diverse, moderate, and non-inflammatory content can only be a good thing, given that algorithms have been directly tied to radicalization and societal harm. But permitting platforms to require that their users submit to the effects of recommendation algorithms is a demonstrable national security risk.

iv. Around 2015, adversaries exploited weaknesses in algorithms and recommendation engines to undermine the United States government and directly target American citizens.

That the majority of Americans and Europeans use social media and the internet for hours each day, pouring personal data into the servers of internet platforms, made social media and the internet ripe vectors for active measures attacks at key moments since 2015, including the 2016 and 2020 elections and the COVID epidemic, the United Kingdom's Brexit referendum, and European elections. In 2017, Facebook disclosed it knew of 470 ads displayed to Facebook users between 2015 and 2017, at a cost of $100,000 to the Kremlin.[52] But Facebook didn't realize the full scope of the manipulation.

In 2020, the bipartisan Senate Select Committee on Intelligence report on Russian active measures during the 2016 election concluded that Kremlin actors "took advantage of the Facebook recommendation algorithm, an assessment Facebook officials have corroborated."[53] The cost was not $100,000 and 470 ads—it was a "multi-million dollar, coordinated effort" to influence the election, costing over a million dollars a month, reaching up to 20 to 30 million Americans each

[47] Florian Saurwein & Charlotte Spencer-Smith, *Automated Trouble: The Role of Algorithmic Selection in Harms on Social Media Platforms,* 9 MEDIA AND COMMC'N (ISSUE 4) 222, 222-233 (2021).
[48] *See infra* pp. 17, 28.
[49] Saurwein & Spencer-Smith, *supra* note 47, at 229.
[50] Granted, a chronological listing may technically be described as an algorithm. But it is a simple by-date sorting algorithm, and involves no machine learning content-assessment or personalization to tailor content to the user. *See* Guess, *supra* note 43, at 398.
[51] Tobias Konitzer et al., *Comparing Estimates of News Consumption from Survey and Passively Collected Behavioral Data,* 85 PUB. OP. Q. 347, 364 (2021).
[52] Scott Shane & Vindu Goel, *Fake Russian Facebook Accounts Bought $100,000 in Political Ads,* N.Y. TIMES (Sep. 6, 2017), https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html.
[53] S. SELECT COMM. ON INTELLIGENCE, 116TH CONG., 1ST SESS., REP. ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, VOL. 2: RUSSIA'S USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS, 47 (Comm. Print 2020).

month.[54] Facebook's estimate is that up to 126 million Americans came into contact with Kremlin-produced content between 2015 and 2017.[55]

Kremlin-produced "content was 'sometimes recommended when people followed similar pages.'"[56] This was "gaming the algorithm," plain and simple: the Senate report found that the Kremlin "utilized the Facebook platform . . . exactly as it was engineered to be used."[57] The Kremlin manipulated, among many sites, Instagram[58] and YouTube in the same way—using manipulation of Twitter and Facebook to further achieve the "viral" spread of YouTube content.[59]

And the Kremlin gamed Google's search algorithm to elevate extremist and false content during the 2016 election.[60] It devoted an entire department of Yevgeny Prigozhin's Internet Research Agency to algorithmic "search engine optimization" to elevate Kremlin-produced content to the top of users' searches.[61] The Senate Report warned about the future of recommendation and search algorithm-gaming:

> The same bots, trolls, click-farms, fake pages and groups, advertisements, and algorithm-gaming the IRA used to conduct an information warfare campaign can be repurposed to execute financial fraud, stock-pumping schemes, digital advertising manipulation, industrialized marketing of counterfeit prescription drugs, and scaled deceptions that spread malware.[62]

During the COVID pandemic, the Kremlin gamed Twitter to spread disinformation about COVID vaccines. For example, Sputnik reportedly embedded malware in Twitter posts to game the recommendation algorithm, apparently by micro-targeting users that clicked, identifying users interested in vaccine issues, and making more disinformation casting doubt on the efficacy of COVID-19 vaccines appear to those Twitter users.[63]

Other foreign states use similar tactics. Iran and China spread disinformation about COVID to Americans,[64] and paid social media sites to amplify their propaganda, via algorithms, to Americans

[54] *Id*. at 22, 30.
[55] *Id*. at 45.
[56] *Id*. at 48.
[57] *Id*.
[58] *Id*. at 49.
[59] *Id*. at 58-59.
[60] *Id*. at 57-58.
[61] *Id*. at 58.
[62] *Id*. at 75.
[63] U.S. DEPT. OF STATE, GLOBAL ENGAGEMENT CENTER, GEC SPECIAL REPORT KREMLIN-FUNDED MEDIA: RT AND SPUTNIK'S ROLE IN RUSSIA'S DISINFORMATION AND PROPAGANDA ECOSYSTEM 5 (Jan. 2022), https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf (citing Disinformation Research Group, *Vaccine news stories hosting malware disseminated across Spanish-language Twitter,* FEDERATION OF AMERICAN SCIENTISTS (Sep. 23, 2020), https://web.archive.org/web/20210520212527/https://fas.org/disinfoblog/vaccine-news-stories-hosting-malware-disseminated-across-spanish-language-twitter/).
[64] Bret Schafer, et al., *Influence-enza: How Russia, China, and Iran Have Shaped and Manipulated Coronavirus Vaccine Narratives,* GMF ALL. FOR SECURING DEMOCRACY (Mar. 6, 2021), https://securingdemocracy.gmfus.org/russia-china-iran-covid-vaccine-disinformation.

and their own citizens.[65] China's TikTok internet service uses algorithms that recommend radicalizing and extremist content.[66] The sensitive personal data of Americans flows through Chinese servers despite TikTok's repeated denials,[67] and the Director of the FBI testified about national security concerns that China could use TikTok to influence American users or control their devices.[68]

Americans themselves game these algorithmic recommendation systems to push content to unwitting American eyes. In the 2020 election, Americans engaged in "'coordinated inauthentic behavior,' which is a term for networks of fake or suspicious accounts acting in concert."[69] In the past, domestic extremists used these tactics against Americans. For example, trial testimony from a domestic extremist revealed the use of coordinated "hashtag" Tweets on Twitter to "hijack[] Twitter's algorithm," capture spots on the "trending lists" algorithm, and thus force-feed far-right content to millions of Americans.[70]

v. Social media and search engine manipulation has a real-world impact: It caused protests during the 2016 American election, riots in Germany, unrest in Canada, made millions disregard medical advice, and affected how people vote.

The real-world impacts of domestic and foreign internet searches and social media manipulation are hotly debated but hidden in plain sight. They are backed up with enough data that no one can deny the effects with a straight face. Kremlin manipulation of American social media during the 2016 election led Americans to physically leave their homes, travel to specified locations, and engage in at least 130 real-world protests across America. These protests were promoted by thirteen Facebook pages run by the Kremlin, with over 60,000 Facebook users indicating they would attend, and promoted overall to almost 350,000 Facebook users.[71] In Germany, Kremlin

[65] Casey Newton, *China is the latest superpower to get caught waging a disinformation campaign on Twitter,* THE VERGE (Aug. 20, 2019), https://www.theverge.com/interface/2019/8/20/20813046/china-disinformation-campaign-hong-kong-twitter-facebook (citing Sophia Ignatidou, *The weaponization of information is mutating at alarming speed,* THE GUARDIAN (Aug. 19, 2019, 4:00 AM), https://www.theguardian.com/commentisfree/2019/aug/19/weaponisation-of-information-mutating-privacy).

[66] Olivia Little & Abbie Richards, *TikTok's Algorithm Leads Users from Transphobic Videos to Far-Right Rabbit Holes,* MEDIAMATTERS (Oct. 5, 2021, 9:03 AM), https://www.mediamatters.org/tiktok/tiktoks-algorithm-leads-users-transphobic-videos-far-right-rabbit-holes; Nikita Aggarwal, et al., *#Fintok and Financial Regulation,* 54 ARIZ. ST. L. J. 1035, 1056 (Winter, 2022), (over 60% of videos shared are memes, and as "TikTok uses an algorithmic recommender system," TikTok uses likes—which could be inauthentic likes "gaming the system"—to "determine[] how to recommend videos to whom.").

[67] Dan Milmo, *TikTok's Ties to China: Why Concerns Over Your Data Are Here to Stay,* THE GUARDIAN (Nov. 8, 2022, 1:00 AM), https://www.theguardian.com/technology/2022/nov/07/tiktoks-china-bytedance-data-concerns.

[68] Rachel Treisman, *The FBI Alleges TikTok Poses National Security Concerns,* NPR (Nov. 17, 2022), https://www.npr.org/2022/11/17/1137155540/fbi-tiktok-national-security-concerns-china.

[69] Kevin Roose, et al., *Tech Giants Prepared for 2016-Style Meddling. But the Threat Has Changed.,* N.Y TIMES (Sep. 22, 2020), https://www.nytimes.com/2020/03/29/technology/facebook-google-twitter-november-election.html.

[70] Michael Edison Hayden, *What We Know About 'Microchip,' The FBI's Far-Right Judas,* S. POVERTY L. CTR. (June 28, 2023), https://www.splcenter.org/hatewatch/2023/06/28/what-we-know-about-microchip-fbis-far-right-judas (quoting testimony Mackey explaining how Microchip and his far-right allies gamed Twitter's algorithm).

[71] S. COMM. ON INTEL., 116TH CONG., REP. ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION 46-47 (2020).

disinformation about a rape and kidnapping of a 13-year-old by migrants, which was amplified by YouTube's recommendation algorithm and other social media, resulted in real-world unrest.[72]

Russia and China both gamed Twitter's algorithms in 2020 for several days by co-opting 40% of Russian and Chinese Twitter "trending topics" mentioning ongoing violence in the U.S. that were force-fed to American users; they used fake Tweets portraying the George Floyd protests as unhinged violence, rather than the peaceful protests they largely were.[73] After days of covert Chinese and Russian inflammatory content being algorithmically fed to millions of young Americans through American social media companies, on the sixth day of protests, violence "erupted in cities across the US."[74] Real Americans marched in these protests. But Russia and China provided rallying cries and fighting words, the social media equivalent of guns and ammunition.

In Canada, a "small collection of local conspiracy theorist" truckers were "supercharged by Facebook's algorithm," "blast[ing] out into" users' feeds information about the 2022 "Freedom Convoy"—this resulted in Fox News devoting multiple hours of programming and amplification to American and European audiences by a Facebook group run by far-right US administrators.[75] But the amplification spiral started by Facebook algorithms was not shut down by Canadian authorities before the group raised a real-world amount of almost $10 million.[76] The Freedom Convoy, was, by many accounts, co-opted by an entirely different group of interests on Facebook, including QAnon online groups, neo-Nazis, and white supremacists—all of them "crossed the line" from the amplified online space and joined the truckers on the ground, making it a fundraising event for their own causes.[77] The online world has real-world effects. The online world *is* the real world.

During the COVID pandemic, when scientific voices were most needed, Americans were pummeled with disinformation. Two-thirds of Americans reported seeing pandemic news that seemed entirely made-up.[78] A 2020 study on social media and vaccine hesitancy, aware of Russian and Chinese disinformation gaming American internet algorithms, found both a "significant relationship between organization on social media and public doubts of vaccine safety" and "a substantial relationship between foreign disinformation campaigns and declining vaccination coverage."[79]

[72] *Id.* at 17.

[73] Mark Scott, *Russia and China Target U.S. Protests on Social Media,* POLITICO (June 1, 2020, 4:12 PM), https://www.politico.com/news/2020/06/01/russia-and-china-target-us-protests-on-social-media-294315.

[74] Anthony Zurcher, *George Floyd Death: Violence Erupts on Sixth Day of Protests,* BBC (June 1, 2020), https://www.bbc.com/news/world-us-canada-52872401.

[75] Ryan Broderick, *How Facebook Twisted Canada's Trucker Convoy into an International Movement,* THE VERGE (Feb. 19, 2022, 7:00 AM), https://www.theverge.com/2022/2/19/22941291/facebook-canada-trucker-convoy-gofundme-groups-viral-sharing.

[76] Elizabeth Thompson, *GiveSendGo Defends Decision to Raise Money for Protest Convoy,* CBC NEWS (Mar. 3, 2022, 3:24 PM), https://www.cbc.ca/news/politics/convoy-finance-givesendgo-gofundme-1.6371861.

[77] Chris Stokel-Walker, *The Alt-Right on Facebook Are Hijacking Canada's Trucker Blockade,* WIRED (Feb. 8, 2022, 2:49 PM), https://www.wired.com/story/ottawa-trucker-protest-facebook-alt-right/.

[78] Christina Pazzanese, *Battling the 'Pandemic of Misinformation,'* THE HARV. GAZETTE (May 8, 2020), https://news.harvard.edu/gazette/story/2020/05/social-media-used-to-spread-create-covid-19-falsehoods/.

[79] Dr. Steven Lloyd Wilson & Charles Wiysonge, *Social Media and Vaccine Hesitancy,* BMJ GLOB. HEALTH Oct. 2020 at 1, 1.

Three years later, the rest is history. An online disinformation tsunami flooded Facebook and Twitter, and then America's news websites and popular non-scientist talk show hosts like Joe Rogan and Infowars' Alex Jones, resulting in embarrassingly low vaccine rates, and 63% higher death rate from COVID than other comparable nations.[80] Higher death rates were directly related to the viewing of Fox News anchor Tucker Carlson and Sean Hannity, who spread falsehoods about COVID nonstop for years.[81]

The downwind effect of online disinformation on potential voters is equally unclear. In 2016, most of us were willing to reserve judgment as to whether Russia's all-out information attack on the United States could have shifted votes in Donald Trump's favor. Today, only those who have buried their heads in the sand could doubt the real-world effects of our modern algorithmic online miasma, particularly the effects of what Robert Mueller found to be a "sweeping and systemic" attack on America's election.

Three double-blind studies found that minor changes to an algorithmic search engine's ranking system influenced the decisions of undecided voters by 20%.[82] In 2020, social media misinformation campaigns paired with Twitter and Facebook's algorithmic recommendation engines of the #Sharpiegate hashtag caused virality and led to real-world protestors in Arizona. The #Sharpiegate and Stop the Steal social media campaigns led to real-world protests in large American cities including Washington, DC.[83] And, of course, "Ali Alexander and other right-wing influencers . . . encouraged Trump supporters throughout the country to converge on Washington, DC, to protest in person," and "the President told a crowd of supporters that 'this election was stolen from you, from me, from the country.'"[84] The January 6th insurrection followed shortly after.

The cause of these real-world ills is in part, and sometimes in large part, these ubiquitous addictive recommendation algorithms. Bellingcat, the investigative journalism organization, analyzed far-right chatrooms online and found that YouTube was the most cited reason for members' conversion to far-right beliefs online.[85] If we know that algorithmic recommendation algorithms "supercharge" disinformation's spread around the world, as research and our eyes show, then we must ask if America, and the world, could have been spared the chaos and damage done over the past decade had Congress required internet services to disclose how their algorithms work to users, and offered users the option to escape the online hellscape they cultivate with a wink and a nod. If we trust consumers to make smart choices, we must assume that they will mostly make the right choice—if well-informed, and if given the option.

[80] Benjamin Mueller & Eleanor Lutz, *U.S. Has Far Higher Covid Death Rate Than Other Wealthy Countries,* N.Y TIMES (Feb. 1, 2022), https://www.nytimes.com/interactive/2022/02/01/science/covid-deaths-united-states.html.

[81] Natalie Moore, *Study Finds More COVID-19 Cases Among Viewers of Fox News Host Who Downplayed Pandemic,* WBEZCHI (Apt. 30, 2020, 3:10 PM), https://www.npr.org/local/309/2020/05/04/849109486/study-finds-more-c-o-v-i-d-19-cases-among-viewers-of-fox-news-host-who-downplayed-pandemic.

[82] Evan M. Williams & Kathleen M. Carley, *Search Engine Manipulation to Spread Pro-Kremlin Propaganda,* HARV. KENNEDY SCH. MISINFORMATION REV. Feb. 2023 at 1, 2 (internal citation omitted).

[83] CTR INFORMED PUB, DIGIT. FORENSIC RSCH. LAB, GRAPHIKA, & STANFORD INTERNET OBSERVATORY, THE LONG FUSE: MISINFORMATION AND THE 2020 ELECTION 171-72 (Eden Beck ed., 2021).

[84] *Id.* at 124.

[85] Kevin Roose, *The Making of a YouTube Radical,* N.Y. TIMES (June 8, 2019), https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html.

b. The problem runs to the foundations of our online world.

The scope of the problem is vast. The impacts are real. In comparable situations in the past where commercial nuisance or actual harm affected consumers, Congress acted quickly. But Congress has done nothing in over a decade to protect Americans from algorithmic manipulation, despite clear and growing awareness of the ongoing crisis. Numerous bills have been introduced. But Congress has produced no legislation. Why is that?

i. Mosaic theory: Our most sensitive and private details, hidden in plain sight for foreign spies, marketing firms, and Big Tech.

One problem causing Congress to hesitate is that the law is in flux. It will take years before the Supreme Court's understanding of the technology matches that of everyday users of social media platforms. And even then, the Court is limited by the laws Congress provides. One example of the languid speed of the law is how long it took for the Court to catch up to the world created around 2007, when the presence of Americans' personal data exploded online at the same time as the emergence of recommendation algorithms and smartphones like the iPhone. It took another ten more for the Court to adjust its understanding of the Fourth Amendment.

In 2018, the Supreme Court moved to push one tentative foot of its Fourth Amendment reasonable expectation of privacy doctrine into the modern online world. The Court appeared to endorse what some call the "mosaic theory" in *Carpenter v. United States*—an interest in a privacy right preventing the government from warrantlessly collecting the cell-site location data for 127 days of a user's cell phone, held by a third party, which amounted to "an all-encompassing record of the holder's whereabouts… [and] an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[86]

The importance of the Court's "mosaic theory" discussion is not whether the right is settled or applied more broadly—rather, it is a prime example of how widespread the notion is that our most sensitive data, accumulated on the servers of internet companies, internet service providers, or the government—reveals our most private lives and morally and normatively deserves protection from misuse and bad actors. Social security numbers and biometric data,[87] information about our sex lives,[88] our intellectual exchanges with friends and colleagues,[89] and information about our children, health, finances, credit reports, electronic communications, and education,[90] are all highly sensitive aspects of our lives—and are often accumulated in one place by internet services. Even outside the context of a Fourth Amendment case like *Carpenter,* this information is personal and sensitive.

[86] *Carpenter v. United States,* 138 S. Ct. 2206, 2211-12, 2217 (2018) (internal citation omitted).

[87] *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 248-49, 255-57 (2007).

[88] *See* Paul Ohm, *Sensitive Information,* 88 S. CAL. L. REV. 1125, 1153-54 (2015).

[89] *See* NEIL M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE, 95-108 (2015).

[90] WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW*,* 302-22, 731-883 (2d ed. 2016).

Because of this, foreign governments and criminal groups directly target this sort of data—whether by hacking computers that accumulate it, legally purchasing commercially available data, or simply scraping the publicly available data—and use it to target us, build profiles on us and our friends and family, map network connections, and conduct information operations, coercion, and blackmail.[91] The Kremlin uses American social media sites to conduct aggressive cyber and disinformation campaigns, for example, against United States service members and veterans.[92]

But courts will not and cannot solve the problem. It took over a decade from the invention of the iPhone for the Fourth Amendment to protect a small subset of geolocation data—which is itself but a subset of all online personal data online. Only Congress can choose to protect all the sensitive data of Americans that comprise the "mosaic" of our personal lives, and only Congress can give Americans the choice to opt-out of these personalized algorithms. Until internet services are required to tell Americans how these algorithms affect the news or stories we see, and how they may be used to radicalize us—we cannot make educated decisions about whether to use these recommendation systems.

ii. The Black Box problem: We don't know when we're being manipulated, and companies refuse to explain it to us.

Another problem is that we don't fully understand how frequently, and how, these algorithms affect the content we see in online marketplaces, social media sites, or search engines. Nor do many of the internet platforms that use these algorithms. Our sensitive data, paired with internet service recommendation algorithms and gaming by these bad actors, leads to national security points of failure. In one study, Facebook found that "64% of all extremist group joins are due to our recommendation tools."[93] On YouTube, where around 70% of views are driven by algorithmically recommended content,[94] viewers similarly are steered toward extremist content. Internal debates have raged inside Facebook, often with the platform favoring viral extreme content, and Facebook employees recommending dialing-back recommendation algorithms to slow the spread of misinformation or recommendations to join extremist groups.[95]

Personal data is exploited mercilessly by online platforms as a routine part of their business model. Makers of internet connected devices, social media sites, shopping sites—the "internet economy" writ large—act in their self-interest to keep us "addicted" to their services, and this addiction is undermining the basic American economic model.[96] Strong capitalism depends on customers free to act on their self-interest, with transparent pricing, rational consumers, which results in the

[91] *See e.g.*, Ben Schreckinger, *How Russia Targets the U.S. Military,* POLITICOMAG (June 12, 2017), https://www.politico.com/magazine/story/2017/06/12/how-russia-targets-the-us-military-215247/; JUSTIN SHERMAN, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS: THREATS TO AMERICAN CIVIL RIGHTS, NATIONAL SECURITY, AND DEMOCRACY (2021).

[92] Suzanne Spaulding, et al., *Why the Kremlin Targets Veterans,* CSIS (Nov. 8, 2019), https://www.csis.org/analysis/why-kremlin-targets-veterans.

[93] Hao, *supra* note 7.

[94] Joan Solsman, *YouTube's AI is the Puppet Master Over Most of What You Watch,* CNET (Jan. 10, 2018, 10:05 AM), https://www.cnet.com/tech/services-and-software/youtube-ces-2018-neal-mohan/.

[95] Hao, *supra* note 7.

[96] Maya MacGuineas, *Capitalism's Addiction Problem,* THE ATLANTIC (Apr. 2020), https://www.theatlantic.com/magazine/archive/2020/04/capitalisms-addiction-problem/606769/.

system's ability to—in a perfect world, on its own—produce social good.[97] But addiction is key for the attention-based internet economy. Internet services, like Facebook, Google, and Amazon, that employ user data like interests and demographics to target content, stories, and ads on the individual level.[98]

For reasons including self-interest, retaining competitive advantage over other internet services, because companies view their algorithms as trade secrets, and to prevent gaming of their algorithms, no company has the incentive to voluntarily reveal details about their algorithms to the public or to government bodies, or to explain clearly to users how their personal information results in the personally recommended content they see, or give users a choice to not receive the personally recommended content.[99] At the same time, political campaigns, domestic and foreign bad actors, and others who either understand the algorithms well enough, or strike business deals with the internet giants to target advertising to users based on the data, make unrestrained use of the algorithms to affect the content users see.

As described further below,[100] the EU's recent Digital Services Act[101] requires that internet services make public a "plain and intelligible" explanation of how their algorithmic recommendation systems, search results, trending topics, and similar operations, work, along with a list of the "main parameters" used in recommender systems.[102] Also, as discussed below,[103] bills have been introduced in Congress to require a similar plain English explanation of how algorithms affect recommendations and search results.[104]

But the sheer complexitKy of these algorithms makes it difficult to explain precisely or accurately how they work.[105] That is, as Haochen Sun points out: (a) the inscrutable machine learning process understandable to programmers is difficult to simply and succinctly explain to laypeople, even before explaining how the algorithm interacts with moderation, filtering, paid content, and user profiles; and, (b) any algorithm explanation posted on an internet services' site would fail to

[97] *Id*.

[98] Stuart Minor Benjamin, *The First Amendment and Algorithms*, in THE CAMBRIDGE HANDBOOK OF THE LAW OF ALGORITHMS, 606, 619 (Woodrow Barfield ed., 2020).

[99] Alexander Pirang, *Germany Wants Greater Algorithmic Transparency to Fight Disinformation, But its Approach is Half-Baked,* NET POLITICS (Apr. 11, 2018, 10:00 AM), https://www.cfr.org/blog/germany-wants-greater-algorithmic-transparency-fight-disinformation-its-approach-half-baked; Daniel Maggen, *Law in, Law Out: Legalistic Filter Bubbles and the Algorithmic Prevention of Nonconsensual Pornography,* 43 CARDOZO L. REV. 1747, 1761 (2022).

[100] *See infra* pp. 28-30.

[101] Benjamin Beck, Dr. Ulrich Worm, *EU Digital Service Act's Effects on Algorithmic Transparency and Accountability,* MAYER BROWN (Mar. 27, 2023), https://www.mayerbrown.com/en/perspectives-events/publications/2023/03/eu-digital-services-acts-effects-on-algorithmic-transparency-and-accountability.

[102] Commission Regulation 2022/2065, 2022 J.O. 1 (amending other direction and creating Digital Services Act.

[103] *See infra* pp. 32-36.

[104] Platform Accountability and Consumer Transparency Act, S. 797, 117th Cong. § 3 (2021) (Congress finds a "compelling government interest" in having the public informed about content moderation, and American people "benefit from transparent information about . . . content moderation practices, including . . . amplifying, prioritizing, or deprioritizing"). Notably, the Bill does not, like the enacted EU DSA, actually mandate disclosure—it merely makes a prefatory Congressional "finding."

[105] Haochen Sun, *Regulating Algorithmic Disinformation,* 46 COLUM. J.L. & ARTS 367, 382-83 (2023) (citing Paddy Leerssen, *The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems,* 11 EUR. J.L. & TECH., no. 2, 2020, at 3).

explain how the user's contribution shaped a given recommendation, since the algorithm depends on user input like likes, comments, clicks, and so on.[106]

As Paddy Leerssen describes it, "[t]hese complex interactions between the recommendation algorithm and its users make for a *recursive and unpredictable system,* with the potential for unexpected feedback loops and path dependencies."[107] Because of this unpredictability and mishmash of inputs, platforms have "little opportunity" to address in real time[108] misinformation or harmful content amplified by the algorithm in an unpredictable fashion, perhaps due to user inputs, due to "black box" decisions not predicted by the programmers, or due to gaming of the system by content providers.

When users and content providers "gaming the algorithm" are added to this mix of complex and not-yet-determined variables, the inability of the algorithm's programmers to describe why it produces this or that result at a given time, can result in a "'rabbit hole' of gradually escalating extremism" that is hard to explain in plain English to users in a succinct website disclosure.[109] We should demand internet services provide such disclosures—but we should expect them to fail[110] because the unpredictability of algorithms is not unlike the unpredictability of generative AI[111]—the possibility of gamed and unexpected results is a "risk of the product." Thus while we should require and expect disclosures like we require "cigarettes cause cancer" notices on cigarette cartons, we must also require platforms enable more research so we can better understand why algorithms affect society and behave way they do.

iii. Social Media and Internet Service Lock-in.

Finally, internet platforms give users little ability to leave their products behind for greener pastures, due to their monopolistic structure: users' friends often gather on one platform, like Facebook, TikTok, or the platform we knew as Twitter. Leaving for another platform, without one's online group of friends, is a bitter pill to swallow, just to escape a platform's addictive and harmful effects. Internet services understandably don't want users to stray to other platforms. The anti-competitive accumulation of power in the hands of companies like Amazon, Google, Twitter, Facebook, and others, and their multi-billionaire leaders, has led some to call the early 21st century the age of digital "robber barons."[112]

[106] *Id.* at 382-3 (citing Paddy Leerssen, *The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems,* 11 EUR. J.L. & TECH., no. 2, 2020, at 4-5).

[107] Leerssen, *The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems,* at 4.

[108] CTR INFORMED PUB, *supra* note 83.

[109] Leerssen, *supra* note 107, at 4.

[110] *See, e.g.,* Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence,* 66 UCLA L. REV. 54, 124 (2019) ("few defendants can explain why an algorithmic model predicted recidivism for them without an opportunity to examine why it reached such predictions. Only other humans who understand the programming languages and statistical models that underlie algorithms can pinpoint those errors by examining them.").

[111] Benj Edwards, *Why ChatGPT and Bing Chat Are So Good at Making Things Up,* ARSTECHNICA (Apr. 6, 2023, 3:58 PM), https://arstechnica.com/information-technology/2023/04/why-ai-chatbots-are-the-ultimate-bs-machines-and-how-people-hope-to-fix-them/.

[112] Geoffrey A. Maine, Dirk Auer, *Antitrust Dystopia and Antitrust Nostalgia: Alarmist Theories of Harm in Digital Markets and Their Origins*, 28 GEO. MASON L. REV. 1279, 1300 (2021) (quoting Luigi Zingales, *"The Digital Robber Barons Kill Innovation": The Stigler Center's Report Enters the Senate*, PROMARKET (Sept. 25, 2019),

Self-interest encourages internet services companies to: (a) not provide an option to turn-off the algorithmic recommendation or search engine, fearing exposing users to irrelevant or uninteresting content;[113] (b) not voluntarily disclose the trade secrets of these computer-coded algorithmic engines,[114] and (c) prevent users from easily leaving the site, by making friends lists, messages, groups joined, or other history hard or impossible to port to other sites.[115]

To the latter point, internet services—particularly social media companies—benefit from scale. That is, they benefit from users bringing and keeping their friends' data on the site and recruiting yet more friends to join the site and stay. Internet services have "strong incentives" against data portability, and a strong incentive to accumulate as many users and as much data as possible.[116] All that data is a boon to the social media company's business model and financial bottom line.[117]

In October 2022, billionaire Elon Musk purchased Twitter for $44 billion, taking the social media site private.[118] Shortly after, Musk has made the following notable actions: (a) he made a "For You" algorithmic recommendation feed the primary way of interacting with the site, promoting Tweets from people users don't follow, in the style of algorithmic Facebook and highly addictive TikTok;[119] (b) he re-platformed extremists including neo-Nazis, accused sex traffickers, and January 6th insurrectionists, and Musk himself joined extremists in spreading lies about COVID and hate about transgender people, among other divisive messages;[120] (c) instead of awarding blue profile checkmarks only to bona fide public figures including politicians and celebrities, Musk

https://perma.cc/KHF4-8KVU ("digital platforms play the role of the traditional robber barons, who exploited their position of gatekeepers to extract a fee from all travelers.")); Steven Strauss, *Op-Ed: Is It Time to Break Up the Big Tech Companies?*, LOS ANGELES TIMES (June 30, 2016, 6:00 AM), https://www.latimes.com/opinion/op-ed/la-oe-strauss-digital-robber-barons-break-up-monopolies-20160630-snap-story.html ("we've got the new Robber Barons: Amazon, Apple, Facebook, and Google . . . And about 40% of Americans get at least some of their news via [Facebook].").

[113] Annemarie Bridy, *Remediating Social Media: A Layer-Conscious Approach,* 24 B.U. J. SCI. & TECH. L. 194, 217 (2018).

[114] Sonia K. Katyal, *The Paradox of Source Code Secrecy,* 104 CORNELL L. REV. 1183, 1186 (2019) ("Because their inner workings are often protected as trade secrets, they can remain entirely free from public scrutiny."); Katyal, *supra* note 110, at 123.

[115] Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 910 (2013) (citing Woodrow Hartzog, *Website Design as Contract,* 60 AM. U. L. REV. 1635, 1650-53 (2011) ("This coercion essentially forces users to relinquish control of their personal information, even when they would rather not. Although website users can reject the contract wholesale, the choice becomes meaningless when services, important information, and social networks are only available on a single website. For example, Facebook users cannot re-create their network on a different social network website without convincing the other Facebook users to leave as well.").

[116] Peter Swire, *The Portability and Other Required Transfers Impact Assessment (PORT-IA): Assessing Competition, Privacy, Cybersecurity, and Other Considerations,* 6 GEO.L. TECH. REV. 57, 70 (2022) (internal cite omitted).

[117] *See, e.g.,* Shin-Ru Cheng, *Approaches to Assess Market Power in the Online Networking Market*, 22 COLUM. SCI. & TECH. L. REV. 231, 241-45 (2021) (explaining Facebook's monetization of user data and constant drive to expand the user base against competitors, extending from expanding to new users, to at least 72 acquisitions of competitors, including Instagram, WhatsApp, and many other).

[118] Kate Conger, Lauren Hirsch, *Elon Musk Completes $44 Billion Deal to Own Twitter,* N.Y. TIMES (Oct. 27, 2022), https://www.nytimes.com/2022/10/27/technology/elon-musk-twitter-deal-complete.html.

[119] Kate Conger, *How Elon Musk is Changing the Twitter Experience,* N.Y TIMES (Apr. 7, 2023), https://www.nytimes.com/2023/04/07/technology/elon-musk-twitter-changes.html.

[120] Abigale Subdhan, *Here's how Twitter has changed since Elon Musk took over as CEO,* THE GLOBE AND MAIL (Dec. 22, 2022), https://www.theglobeandmail.com/business/article-twitter-elon-musk-changes/; Charlie Warzel, *Elon Musk is a Far-Right Activist,* THE ATLANTIC (Dec. 11, 2022), https://www.theatlantic.com/technology/archive/2022/12/elon-musk-twitter-far-right-activist/672436/.

permitted anyone to purchase checkmarks—causing a flood of fake accounts and ongoing user confusion about the authenticity of accounts;[121] (d) blocked all links to competition social media sites for two days, then relented to user pressure to reverse the policy;[122] (e) suspended the accounts of journalists who discussed leaving Twitter;[123] (f) restricted non-users' ability to see Twitter content;[124] and, (g) blocked free third party access to Twitter's data, which academics, researchers, and emergency responders, had long depended on for tasks including analyzing how misinformation spreads, and conducting research to improve emergency disaster response.[125]

This is the anti-competitive behavior that free-market advocates aim to discourage, and it's all happening on a site once viewed as a free "Q&A with world experts that never ended" on matters from intelligence reform, to cybersecurity with computer experts, to law with constitutional scholars, to world news with defense and foreign policy experts, but not just that "collection of haphazard groups . . . of experts, but of *people*" of all stripes.[126] Practically speaking, Musk's changes to Twitter have caused users to flee.[127]

But smarter internet services like Facebook, Instagram, TikTok, YouTube, LinkedIn, and other social media sites routinely take essentially the same anti-competitive measures as Musk, without drawing attention to the measures. None of these sites provide "data portability," that has been recommended to enable users to bring their followers and accounts easily from one site to another. None of them disclose details about how their algorithms work. All of them impose algorithmic recommendations by default, and do not clearly label or make it easy to find an option for a raw, non-algorithmic feed. Musk's antics highlight the dangers facing Americans when internet platforms make these decisions with no transparency to Congress and the public—which is the status quo for all of these platforms.

c. What's happening that Americans don't see and can't control.

Not only is the algorithm a non-public "black box" to users of search engines like Google or users of YouTube, Facebook, or TikTok. Foreign governments and technologically-savvy users and content providers "game" the search and recommendation algorithms in ways invisible to the consumers of content, since sites are not required to disclose when an algorithm force-feeds users content, and users are unable, or unaware, of how to "turn off the algorithm."

[121] Conger, *supra* note 119.

[122] Emma Roth, *Twitter Abruptly Bans All Links to Instagram, Mastodon, and Other Competitors,* THE VERGE (Dec. 19, 2:45 AM), https://www.theverge.com/2022/12/18/23515221/twitter-bans-links-instagram-mastodon-competitors.

[123] Chas Danner, *Elon Musk Tried to Ban Leaving Twitter,* INTELLIGENCER (Dec. 18, 2022), https://nymag.com/intelligencer/2022/12/elon-musks-twitter-bans-sharing-links-to-many-competitors.html.

[124] Matt Binder, *Twitter Now Blocks Visitors from Viewing Tweets, and Profiles Unless They're Logged In,* MASHABLE (June 30, 2023), https://mashable.com/article/twitter-force-visitors-login-view-tweets-profiles.

[125] Justine Calma, *Twitter Just Closed the Book on Academic Research,* THE VERGE (May 31, 2023), https://www.theverge.com/2023/5/31/23739084/twitter-elon-musk-api-policy-chilling-academic-research (noting that formerly free access to the API has reportedly increased to $42,000 per month, which is prohibitive for researchers).

[126] Matt Tait, *Twitter Was Special. But It's Time to Leave.*, PWNALLTHETHINGS (Nov. 20, 2022), https://www.pwnallthethings.com/p/twitter-was-special-but-its-time.

[127] Lois Beckett, Johana Bhuiyan, Abene Clayton, Kari Paul, *A Eulogy for Twitter: the Place We Journalists Loved, For Better or Worse,* THE GUARDIAN (July 8, 2023, 6:00 AM), https://www.theguardian.com/technology/2023/jul/08/twitter-demise-journalists-eulogy-threads-app-elon-musk.

i. Search engine manipulation.

When people use internet search engines, primacy matters: in a 2013 study of 300 million search engine clicks, 92% of the clicks came from the first page of search results presented to the user.[128] And 51% of those clicks on that first page of results—were on the first or second result presented to the user.[129] People rarely look at the second page of search results: web traffic from the second page of results drops by 95%.[130] A 2023 study demonstrated that today, the result is the same: the first search result gets 34% of the traffic of the clicks, of all the search results combined; in comparison, the second search result gets half the traffic that the first search result gets.[131] Primacy matters when it comes to web searches.

Foreign governments and other content providers, including domestic violent extremists, "game" search algorithms on Google, Bing, and other sites, by producing content tailored to make it into those top results when Americans search for content. And domestic extremists, knowing Google is better at weeding out misinformation, tell their followers to use DuckDuckGo and other search engines that are less effective at suppressing misinformation, like Bing, Yahoo, and Yandex.[132]

Foreign government and non-state actors, and domestic extremists, game the algorithm using "backlinks" and "keyphrases," which are the parts of content submitted by content providers that search engines use to decide whether to rank that content on the first page of search results, or in the first two search results on that first page.[133] Although search engines don't make their algorithms public, search algorithm manipulation by creating "backlinks" involves hacking webpages, injecting invisible URLs into webpages, and paying third parties to create links to the website intended to be made more prominent in search results.[134]

Search algorithm manipulation by "keyphrases" is even easier, since conspiracy theories have unique phrases associated with them.[135] Foreign or domestic actors gaming algorithms need only make up, or co-opt, phrases that, once amplified and searched for, will easily result in highly ranked search results—the absence of any or many other websites using a given keyphrase, or a "data void," makes achieving prominent search results much easier.[136] For example, "Rothschild criminal" appears in the top three results of Google, DuckDuckGo, Bing, Yahoo, and Yandex;[137] co-opting that topic on social media, then, can easily lead users to a webpage prominently discussing the fake, potentially radicalizing topic.

[128] *The Value of Google Result Positioning,* CHIKITA INSIGHTS (June 7, 2013), https://research.chitika.com/wp-content/uploads/2022/02/chitikainsights-valueofgoogleresultspositioning.pdf.

[129] *Id.*

[130] *Id.*

[131] Owen Fay, *Value of #1 Position on Google—Positional Analysis Study [2023]* (May 6, 2022), https://pollthepeople.app/the-value-of-google-result-positioning-3/.

[132] Williams & Carley, *supra* note 82.

[133] *Id.*

[134] Evan M. Williams & Kathleen M. Carley, *Search Engine Manipulation to Spread Pro-Kremlin Propaganda,* HARV. KENNEDY SCH. MISINFORMATION REV., APPENDIX: DETAILS ON SEARCH ENGINE MANIPULATION AND CO-AMPLIFICATION (Feb. 16, 2023), https://misinforeview.hks.harvard.edu/wp-content/uploads/2023/02/williams_appendix_20230216.pdf.

[135] *Id.*

[136] Williams & Carley, *supra* note 82.

[137] *Id.*

These foreign and domestic actors have also set up "pseudo think tank" websites blending real news with misinformation and propaganda, with pages collectively containing tens of millions of links to Russian pseudo thinktanks like Global Research, Zero Hedge, and the SVR-directed New Eastern Outlook,[138] while concurrently amplifying American right-wing websites like the Heritage Foundation and American Enterprise Institute.[139] This creates a sub-rosa relationship that the algorithm sees, but users do not.

Due to the reliance on algorithmically determined search results by all prominent web search services, along with the opacity surrounding manipulation techniques including gaming, backlinks, and keyphrases, users remain unaware when individual search results are manipulated by external parties, leaving Americans with no means to escape the algorithmic disinformation.

ii. Recommender-system algorithm gaming.

Social media platforms like Twitter, YouTube, and TikTok, face similar vulnerabilities. Data utilized by search engines is similarly used by content recommendation systems like YouTube's Auto-Play, Twitter's Trending Topics, Netflix, Spotify, and Amazon.[140] YouTube, for example, draws on the personal viewing patterns of the user to personalize additional viewing recommendations.[141]

Bing and Google, and many systems, autocomplete text once a user starts to type a query.[142] These auto-suggestions are generated by prior queries entered by other users of the system.[143] While this streamlines the search process, media manipulators gather in large groups or use bots to feed high volumes of search queries into online platforms to "create" results that guide other users towards content serving the manipulators' commercial, political, criminal, or other agendas.[144]

A similar phenomenon happens on YouTube's "up-next" and auto-play features. Given that YouTube's dataset is significantly smaller compared to the reservoirs of data accessible by Bing and Google, gaming YouTube is an even easier proposition.[145] Unlike Bing and Google auto-complete, which is driven by other user's entries, YouTube's algorithm looks for content resembling the current content, and content the algorithm believes will appeal to the user—based on "likes" by the user or similar users, the behavior of other users after watching the same video, comments on the video, user viewing patterns, and other data, to "deeply personalize" the recommendations.[146]

[138] U.S. DEP'T. OF TREAS., TREASURY SANCTIONS RUSSIANS BANKROLLING PUTIN AND RUSSIA-BACKED INFLUENCE ACTORS (Mar. 3, 2022), https://home.treasury.gov/news/press-releases/jy0628.

[139] Williams & Carley, *supra* note 82.

[140] Michael Golebiewski & Dana Boyd, *Data Voids,* DATA & SOCIETY 13, 37 (2019), https://datasociety.net/wp-content/uploads/2019/11/Data-Voids-2.0-Final.pdf.

[141] *Id.* at 40.

[142] *Id.* at 37.

[143] *Id.* at 38.

[144] *Id.* at 39.

[145] *Id.*

[146] *Id.* at 40.

Some of these data points, too, can be "spoofed"—for example, someone may ask a group of people to purposely engage in activity on YouTube to influence these personalized recommendations.[147] Media manipulators may use metadata in uploaded videos to game the personalized recommendations, or may comment on videos to tie them to other content, for example, which will make the personalization algorithm more likely to recommend specific content to a user.[148] Due to coordinated efforts by manipulative groups, such as anti-vaccination groups, Center for Disease Control videos have been displaced by anti-vaccination content in personalized YouTube recommendations.[149]

Similarly, the comment sections of blogs and news sites can be manipulated by online influence operations. In 2021, at least 242 news stories on thirty-two major European websites in sixteen countries—including The Times, Der Spiegel and Die Welt, Le Figaro, and La Stampa—were attacked by Kremlin disinformation campaigns systematically manipulating the comment sections of news articles.[150] By creating "upvotes" or "likes," the Kremlin made it appear that public opinion was pro-Kremlin in the comments to those stories.[151] Kremlin-linked news organizations then reported on the purported "public opinion" in follow-up news stories.[152]

III. <u>Stumbling Toward a Solution</u>

a. Pre-2015 American responses to objectionable propaganda from abroad, and objectionable content online.

Before the social media revolution of Facebook's "News Feed" around 2007, Americans were targeted from afar, and the spread of lies intended to undermine the national security of the United States unfolded gradually, filtering slowly through foreign and less credible newspapers and only occasionally breaking into the mainstream news.[153]

Notable examples of foreign successes were the KGB's Operation Infektion, which began with the KGB's successful placement in July 1983 of a forgery—claiming the Pentagon created the AIDS virus as a biological weapon, and purporting to quote Pentagon and CIA documents—in an Indian newspaper funded by the Soviets.[154] Soviet news then amplified the story as if it was "news,"[155] and later a prominent academic in East Germany picked up and amplified the story[156]—and in

[147] *Id.*
[148] *Id.* at 41.
[149] *Id.* at 42.
[150] *European News Sites Targeted by Pro-Kremlin Propaganda Campaigns, Says Report,* EURONEWS (June 9, 2021, 11:47 AM) https://www.euronews.com/2021/09/06/european-news-sites-targeted-by-pro-kremlin-propaganda-campaigns-says-report.
[151] *Id.*
[152] *Id.*
[153] CHRISTOPHER ANDREW & VASILI MITROKHIN, THE SWORD AND THE SHIELD: THE MITROKHIN ARCHIVE AND THE SECRET HISTORY OF THE KGB, 242-44 (2001).
[154] THOMAS RID, ACTIVE MEASURES: THE SECRET HISTORY OF DISINFORMATION AND POLITICAL WARFARE 301-303 (2020).
[155] *Id.* at 306-307.
[156] *Id.* at 308.

1986, the story appeared in the United Kingdom.[157] Finally, in 1987, Dan Rather read the story on CBS Evening news.[158]

Before the social media revolution where around 70% of the population uses social media, before the "internet age," it took many years to successfully spread disinformation to a target country's populace. Soviet disinformation worked like that: it involved elaborately faked documents and photographs, invented stories submitted to scientific journals and newspapers, and stories passed by face-to-face contact.[159]

i. United States Information Agency (USIA): The American response to Soviet, and foreign, propaganda.

Solutions through the late 1990s were similarly analog. Responding to the false AIDS "biolabs" stories, the Reagan administration used the United States Information Agency (USIA)—created in 1953[160]—and its Voice of America radio, films, exhibitions, and United States Embassy messaging, which the United States used to combat the falsehoods overseas.[161] The AIDS story was finally killed after a face-to face meeting between Presidents Gorbachev and Reagan in 1987.[162]

The USIA recruited European directors to produce news and documentaries about "Western values" like democracy and free trade, and fed stories to foreign reporters about the successes of the Marshall Plan.[163] The USIA played a role combatting Iraqi disinformation during the 1991 Gulf War, but was disbanded in 1999 when it was seen as no longer necessary, given the end of the Cold War.[164]

But few Americans actually encountered Soviet propaganda: aside from the Dan Rather story, little Soviet propaganda reached everyday American ears. Those few it reached, it did its magic: a 1970s Florida State University study found that Americans that listened to Radio Mosco were more open to the Soviet Union's message than average Americans—but since Radio Moscow was only available on shortwave radio in New York and few other stations, it reached less than 2% of Americans in 1966.[165] The USIA's Voice of America, in contrast, reached 23% of the Soviet population in the 1970s, and some studies found up to 40% of adults in the Soviet Union listened to Western broadcasting.[166]

[157] *Id.* at 309.

[158] *Id.* at 309-10.

[159] Nicholas J. Cull, *America's Countering Soviet Disinformation in the 1980s,* EUR. NETWORK REMEMBRANCE & SOLIDARITY 1 (2021), https://hi-storylessons.eu/wp-content/uploads/2021/02/15_N.Cull_Americas-Countering-Soviet-Disinformation-in-the-1980s_EN.pdf.

[160] Emily T. Metzgar, *Seventy Years of the Smith-Mundt Act and U.S. International Broadcasting: Back to the Future?,* CTR. ON PUB. DIPL. 21 (2018), https://hi-storylessons.eu/wp-content/uploads/2021/02/15_N.Cull_Americas-Countering-Soviet-Disinformation-in-the-1980s_EN.pdf.

[161] Cull, *supra* note 159, at 3.

[162] *Id.* at 5.

[163] Jim Rutenberg, *RG, Sputnik and Russia's New Theory of War,* N.Y. TIMES (Sep. 13, 2017), https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html.

[164] Cull, *supra* note 159, at 6.

[165] Rutenberg, *supra* note 163.

[166] *Id.*

How times change. Cold War Soviet propaganda touched 2% of Americans; decades later, the Russian 2016 attack, supercharged by American know-how and algorithms, was instantly force-fed to around 50% of all Americans.[167]

ii. Section 230: Congress' 1996 solution for online speech was to encourage online speech and insulate internet platforms from liability.

Section 230 of the Communications Decency Act was passed in 1996, as Facebook whistleblower Frances Haugen notes, in a world "radically different" from ours—it was passed in a time with "no recommender systems in the world"—indeed, the first online recommender system appeared on Amazon in 1999.[168] Section 230 has two key provisions, which some say "created the internet"[169] that we know today: (1) it says that internet platforms like Facebook, Twitter, and YouTube—that it calls "interactive computer services"—are not the "publisher or speaker" of information on their sites posted by users, called "information content providers";[170] and, (2) it says that internet platforms are not liable for any "good faith" actions they take to restrict access to material the platforms deem objectionable.[171]

The first clause of Section 230 thus requires that defamation suits or legal remedies target the platform users posting objectionable content—and bars suits, in most cases, against internet platforms hosting the content. And the second clause enables internet platforms to engage in content moderation—and bars lawsuits against platforms for their good faith moderation choices consistent with their moderation policies. In 1997, the Fourth Circuit, upholding Section 230 immunity for America Online, noted that while "[it] might be feasible [to hold] the traditional print publisher [liable for the reader letters it publishes], the sheer number of postings on interactive computer services would create an impossible burden in the Internet context."[172] In 1997, there were 70 million internet users[173]—in 2023, there are around 5.18 billion.[174] Effective and accurate mass content moderation—"impossible" in 1997—is more impossible today.

Frustrated about platform immunity in the face of vast floods of disinformation online, and allegations that platforms may not moderate content in a way every user likes, there have been calls to gut Section 230 immunity. But as demonstrated above, we don't yet fully understand how algorithms affect users—indeed, many computer scientists don't understand this. Section 230 may

[167] DiResta, *supra* note 8.

[168] FRANCES HAUGEN, THE POWER OF ONE: HOW I FOUND THE STRENGTH TO TELL THE TRUTH AND WHY I BLEW THE WHISTLE ON FACEBOOK 149 (2023).

[169] Daniel Funke, *What You Need to Know about Section 230, the "Most Important Law Protecting Internet Speech",* POYNTER (Mar. 3, 2021), https://www.poynter.org/fact-checking/2021/what-you-need-to-know-about-section-230-the-most-important-law-protecting-internet-speech.

[170] 47 U.S.C. § (c)(1).

[171] *See id.* at § (c)(2).

[172] *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 333 (4th Cir. 1997).

[173] *The Internet: Evolution and Growth Statistics,* STACKSCALE (May 17, 2023), https://www.stackscale.com/blog/internet-evolution-statistics/#International_bandwidth_usage_by_region_from_2017_to_2022.

[174] Ani Petrosyan, *Global Number of Internet Users 2005-2022,* STATISTA (Feb. 23, 2023), https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

insist that we direct lawsuits against content providers themselves, or that we ask the FTC to regulate Twitter for deceptively moderating content. But nothing about Section 230 directly addresses the entirely distinct problem of scale and speed, of "virality," that is also the "algorithm problem."

b. How the European Union responded to manipulation of online platforms.

i. The EU societal response.

European countries, in proximity to and accustomed to Russia's active measures and propaganda, has a long history of teaching its citizens the skills to critically assess information and be better able to reject manipulative media. A brief sketch of three countries' efforts follows.

After the online misinformation campaigns against the American and French presidential election, the Charlie Hebdo attack in 2015 linked to online conspiracy theories, and violent protests organized using misleading and distorted posts on Facebook and other platforms, the French government funded courses for students on digital literacy.[175] 30,000 teachers are now trained annually to teach digital literacy.[176]

In 2014, two years before the Russian attack on the American election system, Finland began its own initiative to train residents, students, journalists, and politicians, to identify manipulative content online like the "Russian troll army," manipulated media and video, and fake profiles.[177] Finland had educated its citizens to understand Russian propaganda campaigns for over a hundred years—but when Russia invaded Ukraine in 2014, Finland identified the shift from the physical world to online misinformation campaigns.[178]

As in France, the Finnish education system got involved, and in 2016 revamped the "critical thinking curriculum" to help students spot online disinformation, including on YouTube and social media.[179] Finnish journalist Jessikka Aro—who broke news about Yevgeny Prigozhin's Kremlin troll factory,[180] and had a prestigious award for that work rescinded by President Trump's State Department [181] —has called for the "enablers of Russian trolls," "Facebook, Twitter, Google/YouTube," to be regulated.[182] As you'll see below—that's exactly what the European Union did.

[175] Adam Satariano & Elian Peltier, *In France, School Lessons Ask: Which Twitter Post Should You Trust?,* N.Y. TIMES (Dec. 2018), https://www.nytimes.com/2018/12/13/technology/france-internet-literacy-school.html.
[176] *Id.*
[177] Eliza Mackintosh, *Finland is Winning the War on Fake News. What It's Learned May be Crucial to Western Democracy,* CNN (May 2019), https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.
[178] *Id.*
[179] *Id.*
[180] Hilary Rose, *Jessikka Aro, the Journalist Who Took on Russian Trolls,* THE TIMES (May 29, 2019, 12:01 AM), https://www.thetimes.co.uk/article/jessikka-aro-the-journalist-who-took-on-russian-trolls-fv0z5zgsg.
[181] U.S. DEP'T OF STATE, OFFICE OF INSPECTOR GENERAL, REVIEW OF THE SELECTION PROCESS FOR THE INTERNATIONAL WOMEN OF COURAGE AWARD (Sept. 2020).
[182] Mackintosh, *supra* note 177.

Finally, Estonia, which may have the deepest experience fighting online propaganda, was the target of years of Russian cyberattacks, beginning with a massive cyberattack in 2007, and continuing online propaganda campaigns from the Kremlin targeted at ethnic Russians in Estonia.[183] In 2018, manufactured stories on Russian social media spread through Facebook and the Vkontakte social media site, spreading stories targeted at ethnic Russians in Estonia, falsely claiming that ethnic Russians were being assaulted in the Estonian capital.[184] Estonia's volunteer private sector propaganda watchdog groups helped monitor social media, and spurred Facebook to shut down the accounts.[185]

The Estonian Government also has a Global Engagement Center-analog office that monitors Russian media for propaganda narratives.[186] And Estonian high school students must take a thirty-five hour "media and manipulation class" to learn digital literacy.[187] Unlike the United States' fractured federal response to online manipulation and propaganda, the Estonian government has since 2007 provided a coordinated, multistakeholder response to cyberattacks and online propaganda.[188]

ii. The EU's successful legislative approach, but voluntary framework failure.

But societal approaches can only do so much. As the 1997 Fourth Circuit *Zeran* decision notes, the volumes of misinformation produced by millions of users, and many times more individual pieces of content—today billions of users and even more content—is impossible to moderate or control without the assistance of computers. Computers make mistakes. Therefore, any solution must begin by focusing on, ultimately, notice and choice being provided to each user who encounters recommendation algorithms.

In 2016, the EU enacted strong and broad statutory privacy protections in the General Data Protection Regulation.[189] Some states, like Virginia, Colorado, and California, have similarly strong data protection for their citizens.[190] In short, the GDPR defines "personal data" far more broadly than American federal law; the GDPR defines "personal data" as any information relating to an identified or identifiable person.[191] The broad GDPR definition of "personal data" includes

[183] Christa Case Bryant, *Cybersecurity 2020: What Estonia Knows About Thwarting Russians,* CHRISTIAN SCI. MONITOR (Feb. 4, 2020), https://www.csmonitor.com/layout/set/amphtml/World/Europe/2020/0204/Cybersecurity-2020-What-Estonia-knows-about-thwarting-Russians.

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.*

[188] *Id*.

[189] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) 1.

[190] Anne Wright Fiero & Elena Beier, *New Global Developments in Data Protection and Privacy Regulation: Comparative Analysis of European Union, United States, and Russian Legislation,* 58 STAN. J. INT'L. L. 151, 171 (2022).

[191] Council Regulation 2016/679, art. 4(1), 2016 O.J. (L119) 1, 3.

names, location data, IP addresses, cookies, or any other information to directly or indirectly identify an individual.[192]

The 2022 Digital Services Act builds on this protection for "personal data," adding strong notice and choice provisions for users of search engine and social media algorithms.[193] Article 27 of the Digital Services Act requires "Recommender system transparency": platforms using recommendation algorithms for search, social media, or other purposes, must in "plain and intelligible language" provide users with the "main parameters" their algorithms use, along with "any options" for modifying those parameters.[194] Article 27 also requires that platforms make any options to change how content is displayed "easily accessible from the specific section" where content is displayed.[195]

Article 38 of the Digital Services Act requires that "very large online platforms" and "very large online search engines" using personalization algorithms for search and other content, "provide at least one option for each of their recommendation systems" not based on "profiling"[196]—that is, not based on "personal data" used to "analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[197] "Very large" search engines or online platforms are defined as having an average of 45 million monthly users.[198]

The European Union has thus taken strong legislative action against the "enablers of Russian trolls" and the adverse effects of algorithms that Frances Haugen, Jessikka Aro, and countless others, have called for. The EU accomplished this by offering citizens a choice to reject online content specifically targeted at them—that is, to have the option to choose to avoid the adverse effects of personalized recommendation engines, yet still be able to access search results, social media, and other content. How online platforms adjust to these requirements remains to be seen. But most importantly, users now have notice and choice.

Of course, content moderation is an entirely different question than the "black box" operation of algorithms that society, academics, and computer programmers are only beginning to wrap their heads around. On the content moderation front, the EU implemented a voluntary Code of Practice on Disinformation in 2018, with Jack Dorsey's Twitter as one of the first members.[199] In May 2023—after Elon Musk's purchase, the site of increasing disinformation and propaganda—Twitter withdrew from enforcement of the EU's Code.[200] The Digital Services Act, notably, addresses content moderation issue as well, requiring disclosure of content moderation policies and tools in

[192] See U.K. INFO. COMM'RS OFFICE, GUIDE TO THE GEN. DATA PROT. REGUL. (GDPR), 2018, at 10, (UK).
[193] Regulation (EU) 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L277) 1.
[194] Council Regulations 2022/665, art. 27(1), 2022 O.J. (L277) 1, 59.
[195] Council Regulation 2022/2065, art. 27(3), 2022 O.J. (L277) 1, 59.
[196] Council Regulations 2022/2065, art. 38, 2022 O.J. (L277) 1, 69.
[197] Council Regulation 2016/679, art. 4(4), 206 O.J. (L119) 1, 4.
[198] Council Regulation 2022/2065, art. 38, 2022 O.J. (L277) 1, 63.
[199] *Twitter, Public Health, and Misinformation,* 5 LANCET DIG. HEALTH E328 (June 2023).
[200] Raquel Vazquez Llorente, *How Musk's Twitter is Jeopardizing War Crimes Investigations,* TECHPOLICY PRESS (July 11, 2023), https://techpolicy.press/how-musks-twitter-is-jeopardizing-war-crimes-investigations/.

its terms of service,[201] as well as annual reports on content moderation actions taken[202] and annual risk assessments on their content moderation systems[203]—providing grounds for further enforcement if platforms violate those terms.

c. The United States' response after 2015 mostly came from the private sector. No branch of government has addressed the domestic problem of platform recommendation algorithms.

ii. The American private sector response has been strong, but the private sector cannot force internet platforms to provide transparency or choice.

The "sweeping and systemic" targeting of Americans with algorithmically amplified disinformation came as a shock to the system. Various private sector projects sprang up after the 2016 Kremlin active measures attacks to research, track, and expose social media and online disinformation, including Graphika, Oxford University's Computational Propaganda project, the Atlantic Council's Digital Forensic Research Lab, and others.[204] Internet observatories were set up in universities across the globe, including at Stanford in 2020[205] and Indiana University,[206] to observe trends in the massive amount of digital propaganda flowing across the internet.

Like several European countries, some states have provided an education solution, adopting "digital literacy" curricula for high school students to teach students to identify and assess online propaganda. New Jersey, Illinois, Texas, Washington, Virginia, and Utah, are among the states that have implemented standards for internet literacy, including lessons on how social media works, and how to identify misinformation by cross-checking multiple sources of information.[207] By one 2021 report, since 2015 twenty-eight states had introduced media literacy and digital citizenship bills in their legislatures, and ten states had enacted statutes.[208]

However, research institutions cannot research algorithms if platforms decline to share data with researchers, as happens routinely. Schools cannot educate new citizens if platforms decline to disclose information regarding algorithms or provide choice.

[201] Council Regulation 2022/2065, art. 38, 2022 O.J. (L277) 1, 49.
[202] Council Regulation 2022/2065, art. 38, 2022 O.J. (L277) 1, 49.
[203] Council Regulation 2022/2065, art. 34(2)(b), 2022 O.J. (L277) 1, 69.
[204] Jill I. Goldenziel & Manal Cheema, *The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare,* 22 U. PA. J. CONST. L. 81, 164 (2019).
[205] Stanford Cyber Pol'y Ctr., *The Stanford Internet Observatory Turns Three,* (Jan. 9, 2023), https://cyber.fsi.stanford.edu/news/stanford-internet-observatory-turns-three.
[206] Ind. Univ., OBSERVATORY ON SOC. MEDIA, https://osome.iu.edu/ (last visited Aug. 11, 2023).
[207] David Klepper & Manuel Valdes, *Should Media Literacy Be as Important as Driver's Ed? Some Say Yes.,* THE CHRISTIAN SCI. MONITOR (Mar. 22, 2023), https://www.csmonitor.com/USA/Education/2023/0322/Should-media-literacy-be-as-important-as-driver-s-ed-Some-say-yes; Educ. Comm'n of the States, *Media Literacy & Digital Citizenship*, (2021), https://www.ecs.org/wp-content/uploads/Media-Literacy-and-Digital-Citizenship-PRINTABLE.pdf.
[208] *Id.*

ii. The Global Engagement Center engages in counter-programming, outside the United States, to counter the abuse of American recommendation algorithms by foreigners. It cannot solve the recommendation algorithm problem.

In 2016, to fight propaganda outside the United States, the State Department established the Global Engagement Center, with a mission of "counter[ing] the messaging and diminish[ing] the influence of international terrorist organizations" like ISIL and Al Qaeda.[209] The GEC used social Facebook profile data to target young Muslims showing interest in jihadist causes, "bombard[ing] them with anti-terrorism messages."[210]

The 2017 National Defense Authorization Act statutorily authorized the GEC for an eight year period, provided a robust description of the GEC's duties, and further expanded this mission to lead Federal Government efforts to counter foreign state and non-state propaganda and disinformation.[211] During 2017 under President Trump and Secretary Tillerson, the GEC remained underfunded.[212] And the entire 2017 GEC budget went toward counterterrorism—none of it went toward the new statutory mission that included responding to Russian disinformation.[213]

In 2018, the New York Times reported the State Department had spent none of the $120 million allocated for the GEC since 2016, a claim the State Department disputed, saying the funds were never appropriated.[214] But an audit in 2020 suggests the GEC was funded to almost $100 million in FY 2018, including funds for fighting Russian disinformation.[215] And a 2022 Inspector General report[216] states that the Global Engagement Center, for many reasons, is failing its 2017 tasking[217] to lead federal efforts to "recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation" that undermine national security interests, and its 2021 tasking[218] to "lead and coordinate . . . analytics" into foreign propaganda. Moreover, the GEC's location in the outward-facing Department of State makes it ill-suited, and the wrong body, to address the question of domestic internet platforms recommendation algorithms. That remains squarely the role of Congress.

[209] Exec. Order No. 13,721, 81 Fed. Reg.14,685 (Mar. 17, 2016).

[210] Joby Warrick, *How a U.S. Team Uses Facebook, Guerrilla Marketing to Peel Off Potential ISIS Recruits,* WASH. POST (Feb. 6, 2017, 5:43 PM), https://www.washingtonpost.com/world/national-security/bait-and-flip-us-team-uses-facebook-guerrilla-marketing-to-peel-off-potential-isis-recruits/2017/02/03/431e19ba-e4e4-11e6-a547-5fb9411d332c_story.html.

[211] National Defense Authorization Act for Fiscal Year 2017, Pub. L. 114-328, 130 Stat. 2546, § 1287 (2017).

[212] Robbie Gramer, Ellas Groll, *With New Appointment, State Department Ramps Up War Against Foreign Propaganda,* FOREIGN POL'Y (Feb. 7, 2019, 2:18 PM), https://foreignpolicy.com/2019/02/07/with-new-appointment-state-department-ramps-up-war-against-foreign-propaganda/.

[213] Issie Lapowsky, *The State Department's Fumbled Fight Against Russian Propaganda,* WIRED (Nov. 22, 2017, 6:00 AM), https://www.wired.com/story/the-state-departments-fumbled-fight-against-russian-propaganda/.

[214] Abigail Tracy, *"A Different Kind of Propaganda": Has America Lost the Disinformation War?*, VANITY FAIR, (Apr. 23, 2018), https://www.vanityfair.com/news/2018/04/russia-propaganda-america-information-war.

[215] U.S. DEP'T OF STATE, OFFICE OF INSPECTOR GENERAL, AUDIT OF GLOBAL ENGAGEMENT CENTER FEDERAL ASSISTANCE AWARD MANAGEMENT AND MONITORING (2020).

[216] U.S. DEP'T OF STATE, OFFICE OF INSPECTOR GENERAL, INSPECTION OF THE GLOBAL ENGAGEMENT CENTER 7 (Sep. 2022).

[217] National Defense Authorization Act for Fiscal Year 2017, Pub. L. 114-328, 130 Stat. 2546, § 1287(a)(2), p. 548 (2017).

[218] U.S. DEP'T OF STATE, GLOBAL ENGAGEMENT CENTER, FUNCTIONAL BUREAU STRATEGY 12 (Apr. 30, 2021).

iii. The Supreme Court declined to answer if 230 immunity could be pierced where algorithmic recommendation engines radicalize users. The Ninth Circuit correctly noted that the only solution lies with Congress.

In 2023, the Supreme Court declined to answer the question of whether social media sites can be liable, despite Section 230 immunity, for the "use of powerful algorithms by social media websites [that] can encourage, support, and expand terrorist networks."[219] The Court sidestepped the issue, given that the plaintiffs failed to state a claim for the aiding and abetting that the Ninth Circuit said might escape Section 230 immunity.[220]

But the Ninth Circuit's original opinion correctly notes, given the sea change between the 1980s internet and the internet of 2016 to today, that: (a) "advances in machine-learning warrant revisiting th[e] assumption" at the time Section 230 was enacted that it was "*impossible* for service providers to screen each of their millions of postings"; and, (b) that Section "230(c)(1) shelters more activity than Congress envisioned it would" and that "[w]hether social media companies should continue to enjoy immunity for [all] the third-party content they publish, and whether the use of algorithms ought to be regulated, are pressing questions that Congress should address."[221] Indeed.

More importantly, Section 230 was crafted to address the mundane problem of content moderation. Algorithms require a separate solution, drafted to address the scale and speed of the effects algorithms cause to entire populations—not unlike the solutions Congress drafted decades ago to address the flood of robocalls and junk faxes and spam emails that clogged our phones, fax machines, and email accounts.

iv. The Federal Trade Commission took limited action on social media algorithms, constrained by Congress' failure to act.

The FTC has acted, tentatively. In 2020, the FTC launched a Section 6b study to get "much-needed clarity" into privacy practices at nine social media and streaming companies including Facebook, WhatsApp, Twitter, YouTube, ByteDance, Twitch, Reddit, and Discord, requesting information about those platforms' algorithms.[222] As of 2023, the status of the requests to these nine companies remains unknown.[223] Facebook has, moreover, used possible FTC regulation as its reason to stop sharing data with researchers investigating the spread of disinformation on its platform.[224]

[219] *Gonzalez v. Google LLC*, 2 F.4th 871, 912 (9th Cir,. 2021), *vacated and remanded,* 143 S. Ct. 1191, 1192 (2023).

[220] *Gonzalez v. Google LLC,* 143 S. Ct. 1191, 1192 (2023).

[221] *Gonzalez, supra* note 219, at 1912-13.

[222] Press Release, Federal Trade Commission, Joint Statement of FTC Commissioners Chopra, Slaughter, and Wilson Regarding Social Media and Video Streaming Service Providers' Privacy Practices (Dec. 14, 2020), https://www.ftc.gov/system/files/documents/public_statements/1584150/joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf.

[223] 1 CYBER RISKS, SOCIAL MEDIA AND INSURANCE § 5.04, Lexis+ (database updated 2023).

[224] James Vincent, *Facebook Bans Academics Who Researched Ad Transparency and Misinformation on Facebook,* THE VERGE (Aug. 4, 2021, 11:08 AM), https://www.theverge.com/2021/8/4/22609020/facebook-bans-academic-researchers-ad-transparency-misinformation-nyu-ad-observatory-plug-in.

But as we have seen, these recommendation systems involve complex technical, societal, and legal issues. The Commission has limited powers, and Congress has made no normative statement that uses of algorithms may be "unfair and deceptive trade practices." Internet platforms assert "trade secrets" status over recommendation algorithms, making transparency—without any obvious deception in the algorithm itself—not a clear matter the Commission can resolve. We need to legislate, prescribing notice and consent, and the transparency, that Americans deserve from social media and search platforms. The Federal Trade Commission is the suboptimal place to resolve such issues.

d. Congress' legislative proposals thus far, compared.

The House and Senate have introduced numerous bills that indicate Congress has been unable, yet, to decide what problem is most pressing: providing Americans a choice to avoid algorithmic personalization? Disclosing how user data is used by recommendation algorithms? Providing a public library of advertisements run on platforms? Providing researchers access to data from the platforms, to allow limited study and better public understanding of how the algorithms work?

Many of the below bills have workable language, and the Platform Accountability and Transparency Act has an extremely effective proposal for making platform data to researchers to enable better public, and Congressional, understanding of how platform implementations of algorithms affect us. But none of the proposals clearly provide the urgent basics that America needs now—indeed, that we needed in 2016: (a) to educate Americans about the product and service being provided, and (b) to provide them the basic "choice" that is a staple throughout American consumer law.

Many of these are smart proposals that attack parts of the algorithmic recommendation problem—but few of them tackle the essential protections that the EU partly enacted first in 2016, and then further advanced in 2022: (a) the GDPR's 2016 provision of heightened protection for the "mosaic type" personal information used by online platforms to target users; (b) and, the 2022 DSA's requirement of notice and consent from users about recommendation algorithms; and (c) also in the DSA, mandating a non-algorithmic option. What follows are four notable proposals from Congress.

i. Filter Bubble Transparency Act.

In 2019, a bipartisan group of Senators introduced the Filter Bubble Transparency Act.[225] For large internet platforms, including websites, applications, and other online services,[226] the bill would have (a) required those platforms to clearly notify users at least once that the platform uses an algorithm to "select the content the user sees" "based on user-specific data,"[227] and (b) required those platforms to provide users a clear and persistent way to "switch" that algorithm off, so the user can see content on the service listed in a way that is not affected by "user-specific data"—which the Act calls an "input-transparent algorithm."[228]

[225] Filter Bubble Transparency Act, S. 2024, 117th Cong. (2021).

[226] *Id.* § 2(4).

[227] *Id.* § 3(b)(1)(A).

[228] *Id.* § 3(b)(1)(B).

The bill would have barred platforms—without providing this persistent choice—from displaying data based on an "opaque algorithm," which displays data based on "history of the user's connected device, including . . . web searches and browsing, geographical locations, physical activity, device interaction, and financial transactions" and "inferences about the user or the user's connected device."[229]

However, the bill excepts from this new rule, and thus always permits internet services to display, content based on "user-supplied search terms, filters, speech patterns . . . , saved preferences, and the user's current geographical location"[230] and based on "data supplied . . . by the user . . . such as . . . social media profiles the user follows, the video channels the user subscribes to, or other sources of content on the platform the user follows.."[231]

Violations of the Act would be treated as unfair or deceptive acts or practices under the Federal Trade Commission's jurisdiction.[232]

But the bill: (a) did not alter Section 230 immunity for online interactive computer services; (b) did not require platforms to describe how the algorithm works; (c) did not require algorithmic transparency for academics or other researchers; and (d) did not prohibit algorithmic manipulation other than the specifically listed—that is, it did not require internet services to provide an algorithm-free display of content to users.[233]

ii. Algorithmic Justice and Online Platform Transparency Act.

In 2021, a group of Democratic Senators introduced the Algorithmic Justice and Online Platform Transparency Act.[234] An identical bill was introduced by Democrats in the House.[235] The bill was re-introduced in 2023.[236]

The bill would have required online platforms to do the following: (a) notify users of what personal information is collected and how it is used in the platform's algorithms;[237] (b) notify users of how algorithms recommend, rank, or withhold content when displaying it to users;[238] (c) retain records for five years about the use of personal information by algorithms and how the algorithms work;[239] (d) clearly notify users of content moderation practices;[240] (e) publish an annual "transparency report" on content moderation practices;[241] (f) take "reasonable steps" to make a publicly available

[229] *Id.* § 2(5)(C)(iii)-(iv).
[230] *Id.* § 2(5)(C)(i).
[231] *Id.* § 2(5)(C)(ii).
[232] *Id.* § 4(a).
[233] Adi Robertson, *The Senate's secret algorithms bill doesn't actually fight secret algorithms,* THE VERGE (Nov. 5, 2019, 2:01 PM), https://www.theverge.com/2019/11/5/20943634/senate-filter-bubble-transparency-act-algorithm-personalization-targeting-bill.
[234] Algorithmic Justice and Online Platform Transparency Act, S. 1896, 117th Cong. (2021).
[235] Algorithmic Justice and Online Platform Transparency Act, H.R. 3611, 117th Cong. (2021).
[236] Algorithmic Justice and Online Platform Transparency Act, H.R. 4624, 118th Cong. (2023).
[237] S. 1896, 117th Cong. § 4(a)(1)(A)(i)-(iii) (2022).
[238] *Id.* § 4(a)(1)(A)(iv).
[239] *Id.* § 4(a)(2)(A).
[240] *Id.* § 4(b)(1).
[241] *Id.* § 4(b)(2).

library of advertisements displayed on the platform for the past two years, including information about the advertiser and any targeting criteria;[242] (g) permit users to easily access their personal information and transfer it to other online platforms;[243] and (h) made unlawful the use of algorithms, personal information, or other design features to discriminate, deny equal protection, or impair voting rights, or use algorithms in a "manner that is not safe and effective."[244]

Violations of the Act would be unfair or deceptive acts or practices under the Federal Trade Commission's jurisdiction.[245] The bill explicitly left untouched Section 230 immunity.[246]

Nothing in the Algorithmic Justice and Online Platform Transparency Act requires platforms to give users the choice to "opt out" of algorithmic results or otherwise apply minimally personalized algorithmic results to the content users see on the platform.

iii. Platform Accountability and Transparency Act.

In 2022, a bipartisan group of Senators introduced the Platform Accountability and Transparency Act.[247] The bill was re-introduced in 2023, among other modifications, after removing a provision in the 2022 bill that had created an exception to Section 230 immunity for platforms that failed to comply with the Act's provisions, and removing a provision that would have enabled the Federal Trade Commission to bring civil injunctions against researchers that violate the Act.[248]

In June 2023, a bipartisan group of Senators re-introduced the Platform Transparency and Accountability Act, which has three main parts: (a) independent researchers could submit proposals to the independent National Science Foundation, which if approved would require social media companies to provide data to researchers, with strict privacy protections;[249] (b) it requires social media platforms to make information available to the public, including a library of advertisements, statistics about content moderation, real time data about viral content, and plain language explanations of the algorithms the platform uses for ranking and recommendation;[250] and (c) protection for researchers from legal liability for collection of public platform information.[251]

Platform and researcher failure to comply with some portions of the Act would be unfair or deceptive acts or practices under the Federal Trade Commission's jurisdiction.[252]

[242] *Id.* § 4(c).
[243] *Id.* § 5.
[244] *Id.* § 6.
[245] *Id.* § 8.
[246] *Id.* § 6(i)(4).
[247] Platform Accountability and Transparency Act, S. 5339, 117th Cong. (2022).
[248] Platform Accountability and Transparency Act, S. 1876, 118th Cong. (2023).
[249] *Id.* § 3-4 (2024).
[250] *Id.* § 9 (2024).
[251] *See Senator Coons, colleagues introduce legislation to increase transparency around social media platforms* (June 8, 2023), https://www.coons.senate.gov/news/press-releases/senator-coons-colleagues-introduce-legislation-to-increase-transparency-around-social-media-platforms; Platform Accountability and Transparency Act*, supra* note 248, at § 8.
[252] S. 1896, 117th Cong. § 7 (2022).

Nothing in the present version of the Platform Accountability and Transparency Act changes Section 230 immunity or requires platforms to give users the choice to "opt out" of algorithmic results or otherwise require that users be able to choose to see minimally personalized algorithmic content on the platform.

iv. Platform Accountability and Consumer Transparency Act.

In March 2021, the Platform Accountability and Consumer Transparency (PACT) Act was introduced.[253] The bill was re-introduced in 2023.[254] The bill proposed a Congressional finding that the "people of the United States benefit from transparent information about the decisions interactive computer service providers make regarding . . . amplifying, prioritizing . . . . information."[255]

The PACT Act's three key provisions require interactive computer services: (a) to publish, and make easily acceptable for users, an acceptable use policy, including how content moderation occurs, how users can complain about policy-violating content, as well as how to access the service's biannual transparency report about actions taken to enforce its policy;[256] (b) to set up an easily accessible complaint processing system so users can track processing of complaints;[257] (c) to follow a statutorily prescribed process and timelines for responding to complaints, handling appeals, and notifying content providers about content removal;[258] (d) to provide a process to notify information content providers—that is, often, users—of reasons for removing their content and how to appeal the decision; and, (e) biannually, interactive computer services must publish a "transparency report" disclosing how much content was flagged internally or due to user complaints as violative of policy, and the number of times action was taken for "content deprioritization."[259]

Interactive service provider failure to comply with some portions of the Act are unfair or deceptive acts or practices under the Federal Trade Commission's jurisdiction.[260] In some ways, this bill does the least to help users see how algorithms affect their online experience, and escape from algorithmic results. Instead, the bill focuses on content moderation, which except for the volume of traffic, presents similar challenges to internet platforms as in 1997 when Section 230 was passed.

[253] Platform Accountability and Consumer Transparency Act, S. 797, 117th Cong. (2021).
[254] Platform Accountability and Consumer Transparency Act, S. 483, 118th Cong. (2023).
[255] S. 797, 117th Cong. § 3(5) (2022).
[256] S. 483, 118th Cong. § 5(a).
[257] *Id.* § 5(b).
[258] *Id.* § 5(c).
[259] *Id.* § 5(a)(1), 5(c), 5(d).
[260] *Id.* § 5(g).

e. The self-inflicted national security risk is our unsolved "filter bubble" algorithmic personalization problem. Congress should require platforms provide information to users and researchers about the algorithm and platform use of personal data used, and require a "killswitch" for personalized results.

What values must guide regulation of the algorithms that infect our daily lives? They should be drawn from the deep well of values that have informed regulation of technology in the past. First, we must at minimum provide the "notice and choice" to consumers that the Federal Trade Commission has said are the "core principles of privacy protection."[261] The Commission states that these two principles are the most firmly entrenched values: "choice" is "the most fundamental principle" because "without notice, a consumer cannot make an informed decision";[262] and "choice" is critical, so consumers can decide "how any personal information collected from them may be used."[263] Consumers should be informed every time algorithms use invisible data about their behavior, or the behavior of others, to decide what data they see. And consumers should be given the choice, every time, to "switch it off" and see non-personalized content—that is, see content unaffected by their personal characteristics or the personalized characteristics of others.

Second, we should be guided by the dual and opposing problems that (a) computer experts often cannot explain the input and output effects of algorithms, and that (b) consumers often don't read or understand disclosures and terms of service. These dilemmas push in opposite directions, making the risk of lack of understanding greater when it comes to algorithms.

Because of the documented risk of harm caused by algorithms, the duty of policymakers to everyday Americans is heightened. That is, we must do more given that we cannot explain exactly how or whether a given person will be radicalized, driven to self-harm, driven to avoid vaccines or take untested medicines, driven away from their family members and friends, or otherwise adversely effected by the operation of algorithms in recommendation engines and search results.

Due to the provable link between cigarette use and lung cancer, courts routinely uphold compelled disclosures on every cigarette carton.[264] The Environmental Protection Agency's Toxics Release Inventory—a mandatory disclosure requirement for releases of toxic chemicals by manufacturing and industrial facilities—plays a "central role in driving improvements in pollution performance."[265] Countless other areas in American law require mandatory disclosures: food nutrition; fuel economy; hospital quality; mortgages; securities; sex offenders; tire safety; workplace chemical exposure; and many other products and services.[266]

[261] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1988).
[262] *Id.* at 7.
[263] *Id.* at 8 (citations omitted).
[264] Caroline Mala Corbin, *Compelled Disclosures,* 65 ALA. L. REV. 1277, 1311 (2014).
[265] Bradley C. Karkkainen, *Information as Environmental Regulation: TRI and Performance Benchmarking, Precursor to a New Paradigm?*, 89 GEO. L.J. 257, 286-287 (2001).
[266] Nathan Cortez, *Regulation by Database,* 89 U. COLO. L. REV. 1, 4-5 (2018) (describing the proliferation of data linked to these required disclosures, suggesting how policymakers should deal with this, and noting, at 87, that: "For disclosure policies to succeed on multiple levels, then, they must affect not only the decision-making of consumers and regulatory beneficiaries, but also the decision-making of the discloser—the regulated party.").

Third, Congress must create an accountability and responsibility scheme for internet services that matches the magnitude of societal harms that these algorithmic recommendation systems demonstrably pose to society. Statutory schemes impose costs for non-compliance. But social media, search engine, and internet service recommendation algorithms, do not just overcharge one person in the purchase of a house, and do not misadvise one person about the risks of a medication. Instead, they impact millions, or hundreds of millions, of Americans.

Algorithms make people join ersatz activist organizations and physically protest each other, risking confrontation with each other and police—induced by covert foreign or domestic accounts that social media companies cannot consistently catch before real harm occurs. Algorithms make disinformation about vaccines "go viral," resulting in hospitalization and death. The accountability and responsibility scheme, thus, should be tailored in light of the vast societal harm caused by the algorithms of huge internet companies that serve large parts of, or the majority of, the American population.

Fourth, given the complexity of how algorithms affect our interaction with the online world and the difficulty consumers and platforms alike have understanding that complex relationship, Congress must maximize the opportunity for experts to throw their analysis into the public space, to deepen the conversation and broaden the possibilities for the public to understand the invisible mechanisms that connect us to each other and to the world online.

As Renee DiResta writes, in support of increasing the study of how disinformation, extremism, and propaganda spreads online: "We presently don't know enough about how people believe and act together as groups, or how beliefs can be incepted, influenced or managed by other people, groups or information systems."[267] Until we can understand these systems, we must focus on giving Americans the choice to not be subject to this invisible manipulation, yet still maintain their access to information and their friends online. We should shift our immediate attention from content moderation and vast rewrites of Section 230, to providing Americans notice, choice, and mechanisms to start to better understand algorithms and their bad effects.

f. Legislation has successfully tackled similar problems in the past.

Congress has faced similar problems before, providing models for legislation addressing the glut of un-asked for content "recommended" and forced to our phones, our phones, and our televisions. In the 1990s, Congress legislated to protect consumers from the flood of robocalls. And a decade later, with the surge in use of email, Congress legislated to regulate spam emails. Both are close analogs to our current flood of commercial algorithms.

[267] Renée DiResta, *How Online Mobs Act Like Flocks of Birds,* NOEMA (Nov. 3, 2022), https://www.noemamag.com/how-online-mobs-act-like-flocks-of-birds/.

i. Telephone Consumer Protection Act of 1991: How Congress addressed robocalls and "spam" faxes by providing multiple enforcement mechanisms, enabling "bounties" against offenders.

The Telephone Consumer Protection Act of 1991 ("TCPA") was passed after over forty states had already acted to regulate phone calls to consumers from autodialers and prerecorded messages, after receiving complaints from consumers.[268] Congress acted (1) to address "voluminous consumer complaints about abuses of telephone technology . . . [including] computerized calls dispatched to private homes" and (2) to "prevent businesses from shifting their advertising costs" to the recipients of unsolicited fax advertisements.[269] By 1991, telemarketing calls generated $435 billion in sales annually.[270]

The TCPA regulated "robocalls" by (1) banning robocalls, but letting the Federal Communications Commission create exemptions,[271] (2) requiring that calls automatically disconnect from consumers' phones within five seconds of the consumer hanging up,[272] and (3) requiring all prerecorded unsolicited calls to, at the beginning of the call, clearly state the identity of the called, and the caller's phone number address during or after the message.[273] The TCPA completely banned unsolicited fax advertisements, given the cost to consumers to receive faxes.[274]

The TCPA is enforced in three ways: (1) consumers have a private right of action in state court for injunctive relief, and to sue for $500 per violation, or actual monetary loss, whichever is greater, with treble damages for knowing and willful violations;[275] (2) state officials may bring civil lawsuits in federal District Court for damages and injunctive relief if the case involves a "pattern or practice of violations," for the same range of penalties per violation as in the private right of action;[276] and (3) the FCC may seek forfeitures of $16,000 per violation of the TCPA.[277]

Courts have upheld the lawfulness of these private awards of damages despite that the violations cause "little measurable injury," and that "Congress is permitted to create legally enforceable bounty systems for assistance in enforcing federal laws, provided the bounty is a reward for redressing an injury of some sort (though not necessarily an injury to the bounty hunter)."[278]

The TCPA proved effective at its original purpose: reducing unwanted telemarketing calls and junk faxes.[279] New technology including cell phone number spoofing and text message spam created

[268] Spencer Weber Waller et al., *The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology*, 26 LOY. CONSUMER L. REV. 343, 354-355 (2014).
[269] *Id.* at 355 (citing *Critchfield Physical Therapy v. Taranto Grp., Inc.,* 263 P.3d 767, 774 (Kan. 2011) (citing *Phillips Randolph v. Adler Weiner Research Chicago*, 526 F. Supp. 2d 851, 852 (N.D. Ill. 2007))).
[270] *Id*. at 353.
[271] 47 U.S.C. § 227(b).
[272] In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 7 FCC Rcd. 8752, 8778 § 52 (Oct. 16, 1992).
[273] *Id.* at 8778 § 53.
[274] *Id.* at 8779 § 54 n.87.
[275] 47 U.S.C. § 227(b)(3).
[276] *Id*. § 227(g).
[277] *Id*. § 503; Waller, *supra* note 268, at 404.
[278] *Crabill v. Trans Union, LLC,* 259 F.3 662, 665 (7th Cir. 2001).
[279] Waller, *supra* note 268, at 374.

challenges for the statue, leading to amendments in 2010 to address number spoofing.[280] The private right of action has been an effective deterrent.[281] State attorneys general proved willing to bring TCPA actions, including a 2003 suit by California seeking $15 million in penalties.[282] On the other hand, some recommend that (1) the damages state attorneys-general may seek should be increased to further incentivize state use of the TCPA, and (2) the FTC should also be empowered to bring suit under the TCPA—rather than just the FCC, which is the primary agency for the TCPA.[283]

The TCPA is a useful model for any law regulating commercial personalized algorithms affecting Americans. The TCPA regulates unsolicited phone calls and faxes, which cost consumers: this is similar to commercially-driven algorithmic content, pushed onto consumer screens in ways that sometimes harm Americans, causing violence, suicide, addictive behavior, among many harms caused by algorithmic personalization. The TCPA also provides a useful tripartite enforcement mechanism for consumers seeking relief, state attorneys-general, and a federal agency like the FCC or FTC. This monetary relief in turn incentivizes compliance by commercial actors.

ii. The CAN-SPAM Act of 2003: Inspired by the TCPA, Congress acted against new technology-related nuisance, "email spam," creating multiple enforcement mechanisms and criminalizing some email spam-related acts.

The CAN-SPAM Act of 2003 was passed after thirty-seven states already had enacted anti-spam laws to prevent the spread of commercial email advertising and unsolicited pornography.[284] The CAN-SPAM Act regulated the newest proliferation of unwanted commercial communications, commercial email, or "spam." Unlike the TCPA, which bans unsolicited faxes, the CAN-SPAM Act only regulates a subset of commercial emails.[285] The CAN-SPAM Act prohibits three types of commercial emails: (a) emails with materially false or misleading sender, header, or "from" line information;[286] and (b) emails with false subject line information.[287]

The CAN-SPAM Act requires commercial emails to "clearly and conspicuously" provide notice, and directions, for how email recipients may opt-out of receiving future commercial emails.[288] It prohibits the sending of commercial electronic messages to consumers after consumers have objected.[289] And it prohibits sending any commercial email without notice on how to opt-out.[290]
Unlike the TCPA, the CAN-SPAM Act creates no private right of action. Instead, violations of the CAN-SPAM Act are enforced by the Federal Trade Commission as unfair deceptive acts or

[280] *Id.* at 394-95, 397.
[281] *Id.* at 400-01.
[282] *Id.* at 403-04.
[283] *Id.*
[284] *Id.* at 361.
[285] CAN-SPAM Act, 15 U.S.C. § 7701 et seq.
[286] 15 U.S.C. § 7704(a)(1).
[287] 15 U.S.C. § 7704(a)(2).
[288] 15 U.S.C. § 7704(a)(3)(A)(i).
[289] 15 U.S.C. § 7704(a)(4).
[290] 15 U.S.C. § 7704(a)(5).

practices.[291] It allows for civil actions to be brought by Internet Service Providers to enjoin further violations or for actual monetary loss, or statutory damages in the amount of up to $250 per violating message received—including treble damages for willful and knowing violations.[292] And it allows civil actions to be brought by state attorneys general to enjoin further violations, or, for the greater of actual monetary loss, or statutory damages as described above.[293] Finally, the CAN-SPAM Act criminalizes the sending of sexually oriented material directly to consumers, under Title 18, subject to five years imprisonment or a fine.[294]

Most successful actions under the CAN-SPAM Act have been FTC actions: for example, a $900,000 settlement in 2006 paid for sending consumers commercial emails disguised as personal emails, with misleading subject lines; a 2008 settlement of almost $3 million for commercial emails sent with deceptive subject lines.[295] Internet service providers' right of action has also been successful,[296] provided they prove that their business was "adversely affected"[297] by the CAN-SPAM Act violations. Statutory damages under CAN-SPAM Act—at $250 per violation, and sometimes treble damages—are often higher than actual damages, and "can easily surpass $100 million."[298]

On the other hand, as with the TCPA, new technology requires new approaches: when the CAN-SPAM Act was introduced, 60% of email traffic was spam—by 2010, almost 90% of all global email traffic was spam.[299] Still, targeted enforcement actions against bad actors reachable by the justice system can have beneficial effects.

While CAN-SPAM has been applied to emails sent through social media sites Myspace,[300] search results or social media posts are not good fits for the CAN-SPAM Act. Most online interactions today on social media feeds or search engines cannot be recharacterized as "emails" to fall under the CAN-SPAM Act. Nonetheless, CAN-SPAM provides useful lessons for the algorithmic personalization problem.

Statutory damage remedies, granted to the internet platforms deluged with misleading commercial information, can be incentives to encourage internet service providers to help minimize harmful or misleading content. Content that merely games the algorithm exacts costs on internet platforms and users alike: unhelpful, misleading, extremist content from content providers obfuscates the algorithm's amplification of useful, personalized, non-harmful, and accurate content to users.

Moreover, Congress can designate the FTC as an enforcement mechanism, and statutorily designate misleading commercial emails, and misuse of algorithms by transmitting misleading

[291] 15 U.S.C. § 7706(a).
[292] 15 U.S.C. § 7706(g).
[293] 15 U.S.C. § 7706(f).
[294] 15 U.S.C. § 7704(d).
[295] David Lorentz, *The Effectiveness of Litigation Under the CAN-SPAM Act*, 30 REV. LITIG. 559, 573 n.65 (2011) (internal citations omitted).
[296] *Id.* at 574.
[297] 15 U.S.C. § 7706(g)(1).
[298] Lorentz, *supra* note 295, at 574.
[299] Waller, et al., *supra* note 268, at 343 (internal citations omitted).
[300] *MySpace, Inc. v. Globe.com, Inc.*, No. CV 06-3391-RGK (JCx), 2007 U.S. Dist. LEXIS 44143, at *1 (C.D. Cal. Feb. 27, 2007).

content to "game" algorithms with backlinks or other manipulative content, as "unfair and deceptive practices." This opens the door to enforcement actions based on virality caused by recommendation engines gamed through intentionally deceptive acts. Criminalizing especially injurious unwanted sexual content enables Department of Justice involvement. Finally, an "opt out" provision for consumers enables consumers to express their preference, with another potential violation for senders who ignore consumer choice. "Notice and choice," a range of enforcement options, and involvement by a federal agency, are a time-tested combination.

g. A proposed response—American Algorithmic Choice and Transparency Act.

Frances Haugen, the Facebook whistleblower, has recommended both (a) a targeted exemption to Section 230 for algorithmic ranking, and (b) a return to Facebook's chronological, non-algorithmic, newsfeed.[301] It may be premature to wholly exempt recommendation algorithms from Section 230 immunity at this point, as little to no transparency exists as to how these platforms' algorithms work: that is, excepting algorithms wholly from Section 230 protection would be legislating blind. As Ellery Roberts Biddle, of Ranking Digital Rights, argues, for "such a carve-out to be actionable . . . policymakers and the public would need . . . a much greater level of transparency into how . . . ad-targeting and content-ranking systems . . . work."[302]

Thus, requiring platforms to provide a small group of vetted researchers access to social media data, to study and report on the hard-to-understand "black box" effects of algorithms, would facilitate policymaking and legislation in years to come, as proposed by the Senate's Platform Accountability and Transparency Act bill. I have reproduced and cited to several sections of that bill in my proposed statue. But for now, much can be accomplished with targeted legislation to provide basic notice and choice.

Facebook, Instagram, and Twitter claim to offer non-algorithmic feeds, but in fact those feeds are merely "less algorithmic." Musk's Twitter offers a "non-algorithmic" feed, but it takes at least five steps to enable that option.[303] Instagram's "Posts You've Liked" offers a more-chronological feed, but not a fully chronological feed.[304] Facebook offers no way to completely disable algorithmic recommendations, but users can make the algorithm less prominent.[305]

Sites like YouTube, LinkedIn, TikTok, Netflix, Spotify, and most other social media sites have no non-algorithmic way to interact with their services. For all these services, an algorithmic recommendation engine is either the only option—or is a heavily favored option, and "dialing back" or "turning off" the algorithm rangers from "not easy" to "impossible." One suspects that

[301] Karen Hao, *The Facebook whistleblower says its algorithms are dangerous. Here's why.,* MIT TECH. REV. (Oct. 5, 2021), https://www.technologyreview.com/2021/10/05/1036519/facebook-whistleblower-frances-haugen-algorithms/.
[302] *Id.*
[303] Matthew Lynch, *How to Disable Algorithmic Feeds on Twitter, Instagram, and Facebook,* THE TECH EDVOCATE, (June 23, 2023), https://www.thetechedvocate.org/how-to-disable-algorithmic-feeds-on-twitter-instagram-and-facebook/.
[304] *Id.*
[305] *Id.*

Facebook, Instagram, and Twitter offer these "diet non-algorithmic" options to forestall Congressional regulation of recommendation algorithms.

But algorithms persist on all of these platforms. We do not, and cannot, know how personalized search results and social media feeds are on these platforms—they do not tell us. They do not tell us what personal data they use. Combined with the refusal to share data with researchers, we cannot verify the effect changes in the algorithms have on virality or societal harms, or on the content that displays in personalized feeds.

CAN-SPAM was Congress' answer to new technology—commercial unsolicited emails—bringing nuisances and costs to consumers similar to the commercial robocalls and unwanted faxes that spurred passage of the TCPA. Commercial algorithmic personalization, including search, social media, and music and video content, serves both to "addict" users to a service, and also to make them view more ads or spend more money on a site. The manipulation of the algorithm is the problem we must address. The lessons of TCPA and CAN-SPAM need merely be adjusted to the commercial abuses of this new medium.

The draft bill below borrows language from Section 230, referring to platforms as "interactive computer services," and to those who provide content as "information content providers." The proposal includes the following key provisions:

(1) A requirement for platforms to provide consumers the ability to easily "turn off" personalized algorithms that affect the social media, search, and other online content that they see, and provide users a non-personalized, non-algorithmic way to access content, unique to his proposal, more robust than the Filter Bubble Transparency Act's provisions, but similar to the EU's DSA;
(2) a requirement for platforms to disclose what personalization algorithms they use, how they work, and what data they rely on, similar to other proposals;
(3) a requirement for platforms to provide access to platform data through the "qualified researcher" programs as proposed by the Platform Accountability and Transparency Act;
(4) a limited exemption to Section 230 immunity where platforms fail to reasonably fulfill the Act's algorithmic choice and transparency requirements, unique to this proposal;
(5) a new set of crimes covering commercial information content providers, or content providers in return for money, who knowingly supply misleading information to platforms to intentionally "fool" algorithms into displaying content the algorithm would not otherwise recommend to users—not unlike the crimes created by the CAN-SPAM Act, which addresses analogous email problems—but unique to this proposal; and,
(6) enforcement rights, including a TCPA- and CAN-SPAM-like rights of action for states, consumers, and the FTC, to seek remedies for noncompliance with the provisions of the Act, similar to pending proposals and drawing on past consumer-protection acts of Congress.

I have included key parts of the proposed statute below. Some sections I omit for brevity, and a footnote is provided to direct the reader to model statutory language, including to the superb "qualified researcher" provisions of the proposed Platform Accountability and Transparency Act, and also to relevant analogous provisions in the proposed Algorithmic Justice and Online Platform

Transparency Act, and to the legacy statute, the Telephone Consumer Protection Act of 1991. Some of the language below has been lifted from each of those proposed or current laws, in addition to the unique new provisions described above.

The proposed statute follows:

i. Algorithmic Choice and Transparency Act.[306]

SECTION 1. SHORT TITLE.

This Act may be cited as the "Algorithmic Choice and Transparency Act of 2023," or the "ACT Act of 2023."

SECTION 2. CONGRESSIONAL FINDINGS AND POLICY.

(b) CONGRESSIONAL DETERMINATION OF PUBLIC POLICY.—On the basis of the findings in subsection (a) the Congress determines that—

(1) there is a substantial government interest in regulation of personalized algorithms on a nationwide basis;

(2) providers of internet services should not mislead users as to the reasons content is being provided to, displayed to, or otherwise conveyed to users;

(3) users of internet services have the right to an explanation of the reasons content is being provided to, displayed to, or otherwise conveyed to them by internet services;

(4) users of internet services have a right to decline content that is provided, displayed, or otherwise conveyed to them by a personalized algorithm, including algorithms personalized to the user's data, or personalized to any other user's data;

(5) Internet services have a commercial interest in not publicly releasing details of their algorithms but cannot fully explain why algorithms produce results on either an individual or systemic level;

(6) The public and Congress have an interest in understanding how algorithms affect behavior. Algorithms used by interactive service providers have proven both vastly beneficial, but also exceptionally dangerous. Understanding the effect of algorithms is of critical importance to the Nation, and can be facilitated by a careful partnership between the public, researchers, Congress, and interactive computer services.

[306] A disclaimer: in drafting this proposed statute, my very first draft began with my asking the artificial intelligence platform ChatGPT for a draft bill providing choice and notice to consumers, based on past acts of Congress. I have replaced almost all of the language from that initial draft, stealing portions from other draft bills as noted, and drafting other sections myself. But I have retained the simple ChatGPT definition of "algorithm," and the title provided by ChatGPT—the "Algorithmic Transparency and Choice Act," drawn from the terms of my initial query—I retained and reorganized for its more pleasing acronym. My initial title was "The AOK Act: The Americans' Online Killswitch Act"—which I liked, but may be insufficiently milquetoast for Congress.

SECTION 3. DEFINITIONS.

In this Act:

(1) The term "algorithm" means a set of rules or procedures that a computer program follows to process data or perform a task;

(2) The term "algorithmic ranking" means the use of an algorithm partly or fully by an interactive computer service to determine the order, relevance, prominence, prioritization, or customization of the presentation of content, products, search results, services, or other information presented to a user on an interactive computer service;

(3) The term "algorithmic personalization" means the use of algorithmic ranking to determine the order, relevance, prominence, prioritization, or customization of the presentation of content, products, services, search results, or other information presented to a user of an interactive computer internet service based the automated profiling of on the user's personal data or any other user's personal data;

(4) The term "non-personalized algorithmic ranking" means "algorithmic ranking" that is not a "algorithmic personalization." "Non-personalized algorithmic ranking" includes (a) the chronological or reverse chronological listing of items in the order they were posted online by information content providers; (b) search functions where order, relevance, and customization of the presentation of content, products, services, and other information is directly determined by the terms of the user's current search and no other algorithmic functions; (c) searches, social media, and other displays of content where the user has the ability to select and deselect every item of personal data being used to determine the order, relevance, and customization of the presentation of content, products, services, and other information, and see the immediate effect of those selections and deselections on the display of data;

(5) The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the internet or any other interactive computer service;

(6) The term "interactive computer service" means any information service or system, website, online platform, application, or device that provides or enables computer access by multiple users to a computer server or internet service, or facilitates the transmission or exchange of information over the internet;

(7) The term "personal data" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or consumer device or household. Personal data includes but is not limited to:

a. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;

b. Biometric information;

c. Commercial information, including records of personal property, products, or services purchased, obtained, or considered;

d. Internet or other electronic network activity information including browsing history, search history, and information including a person's interaction with internet websites, applications, or advertisements;

e. Geolocation data;

f. Professional or employment related information;

(8) The term "personal data" does not include publicly available information. Publicly available information under this Act means information lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.[307]

(9) The term "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate, analyze, or predict any person's personal preferences, characteristics, psychological trends, predispositions, behavior, attitudes, interests, economic situation, health, reliability, aptitudes, employment, location, or movements.

(10) The term "qualified data and information" means data and information from an interactive computer service—[308]

(A) That the NSF determines is necessary to allow a qualified researcher to carry out a qualified research project; and

(B) that—

(i) is feasible for the platform to provide;

(ii) is proportionate to the needs of the qualified researchers to complete the qualified research project;

(iii) will not cause the platform undue burden in providing the data and information to the qualified researcher; and

(iv) would not be otherwise available to the qualified researcher.

(C) EXCLUSIONS.—However, "qualified data and information" does not include any of the following:

[307] To reduce information considered "publicly available" for purposes of any statute regulating algorithmic use of personal data with a "publicly available" exception, Congress must take follow-on or concurrent action to reduce the flood of sensitive and personal information online used to target servicemembers, government officials, and everyday Americans—and that is considered "commercially available" for purchase and sale by data brokers, and for purchase by the federal government and other actors. Bills introduced to address this problem include the Data Broker List Act of 2021, S. 2290, 117th Cong. (2021), the DELETE Act, S. 3627, 117th Cong. (2022), and the American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[308] *See* S. 1876, 118th Cong. § 2(6) (2023).

(i) Direct and private messages between users.

(ii) Biometric information, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patters or characteristics.

(iii) Precise geospatial information.

(11) The term "qualified researcher" means a researcher affiliated with a United States university or a United States nonprofit organization (as described in section 501(c) of the Internal Revenue Code of 1986) that is specifically identified in a research proposal that is approved as a qualified research project pursuant to section 7.[309]

(A) However, "qualified researcher" does not include a researcher who is affiliated with a Federal, State, local, or tribal law enforcement or intelligence agency.

(12) The term "qualified research project" means a research plan that has been approved pursuant to Section 7.

(13) The term "NSF" means the National Science Foundation.

(14) The term "user" means any individual who accesses or uses an interactive computer service, including advertisers and sellers.

(15) The term "Commission" means the Federal Trade Commission.

SECTION 4. ALGORITHMIC CHOICE—THE ALGORITHM "KILLSWITCH"

(a) REQUIREMENT TO PROVIDE NON-PERSONALIZED ALGORITHMIC RANKING.—Every time an interactive computer service uses algorithmic personalization to determine the order, relevance, prominence, prioritization, or customization of the presentation of content, products, services, search results, or other information presented to a user, the interactive computer services shall provide at least one non-personalized algorithmic ranking way to view the content, products, services, search results, or information.

(b) ACCESS TO AND USE OF THE NON-PERSONALIZED ALGORITHMIC RANKING FUNCTIONALITY MUST BE PROMINENT AND EASILY ACCESSIBLE.—The internet computer service shall make the option to switch to non-personalized algorithmic ranking of content, search results, or other information, immediately and constantly accessible to users in immediate proximity to where the user is viewing the algorithmically personalized data. Internet computer services shall not require more than one click from a user to switch to a non-personalized algorithmic ranking viewing of content, or to switch back to algorithmic viewing of content.

SECTION 5. ALGORITHMIC TRANSPARENCY.

(a) REQUIRED DISCLOSURE TO USERS.—Beginning 1 year after the date of enactment of this Act, with respect to each algorithmic personalization process, interactive computer services shall disclose to users, in conspicuous, accessible, and plain language that is not misleading:

[309] *See id.* § 2(7).

(1) The categories of personal data that the interactive computer service collects, creates, or uses, for purposes of algorithmic personalization;
(2) The categories of publicly available information that the interactive computer service collects, creates, or uses for purposes of algorithmic personalization;
(3) The manner the interactive computer service uses to collect, create, or use that personal data;
(4) How the interactive computer service uses the personal data and publicly available information for algorithmic personalization;
(5) How the algorithmic personalization process determines the order, relevance, prominence, prioritization, or customization of the presentation of content, products, services, search results, or other information presented to a user.

(b) DISCLOSURE RECORD RETENTION REQUIREMENTS.—Each interactive computer service shall retain records of disclosures to users under paragraph (a) for 5 years.

(c) PROVISION OF QUALIFIED DATA AND INFORMATION.—An interactive computer service shall provide access to qualified data and information relating to a qualified research project to a qualified researcher under the terms and privacy and cybersecurity safeguards dictated by the Commission pursuant to section 7 for the purpose of carrying out the qualified research project.[310]

(d) CONTINUED ACCESS TO QUALIFIED DATA AND INFORMATION.—[311]
(1) In general.—An interactive computer service may not restrict or terminate a qualified researcher's access to qualified data and information for an ongoing qualified research project unless the platform has a reasonable belief that the qualified researcher is not acting in accordance with the cybersecurity and privacy safeguards required for the qualified research project pursuant to section 10.
(2) Notice and Review of Change of Access.—If an interactive computer service restricts or terminates a qualified researcher's access to qualified data and information for an ongoing qualified research project—
(A) the platform shall, within a reasonable time (as established by the Commission, inform the Commission in writing that the interactive computer service has restricted or terminated the qualified researcher's access to the qualified data and information; and
(B) the Commission shall promptly review the interactive computer service's decision and determine whether the qualified researcher has violated the privacy and cybersecurity safeguards established for the qualified research project.

(c) NOTICE TO INTERACTIVE COMPUTER SERVICE USERS ABOUT QUALIFIED RESEARCHER USE OF DATA.—The Commission shall issue regulations requiring that interactive computer services, through posting of notices or other appropriate means, keep users informed of their privacy protections and the

[310] *Id.* § 4(a).
[311] *Id.* § 4(b).

information that the interactive computer service is required to share with qualified researchers under this Act.[312]

(d) INJUNCTIVE RELIEF FOR INTERACTIVE COMPUTER SERVICE FAILURE TO PROVIDE QUALIFIED DATA.—If an interactive computer service fails to provide all of the qualified data and information required under the terms of a qualified research project to the qualified researcher conducting the project, the qualified researcher or the researcher's affiliated university or non-profit organization may bring an action in district court for injunctive relief or petition the Commission to bring an enforcement action against the interactive computer service.[313]

SECTION 6. OTHER PROTECTIONS FOR USERS OF INTERACTIVE COMPUTER SERVICES AND FOR INTERACTIVE COMPUTER SERVICES.

(a) EXEMPTION FROM LIABILITY PROTECTION FOR ALGORITHMIC PERSONALIZED CONTENT SHOWN TO USERS WHEN FAILING TO COMPLY WITH THE ALGORITHMIC CHOICE AND TRANSPARENCY ACT.—Section 230(c) of the Communications Act of 1934 (47 U.S.C. 230(c)) is amended by adding at the end the following:

"(3) Protection Exemption.—

(A) In General.— The protection under paragraph (1) shall not apply to a provider of an interactive computer service with respect to content shown to a user of an interactive computer service by its algorithmic personalization, as defined by the Algorithmic Choice and Transparency Act, if the interactive computer service cannot demonstrate that it has taken all reasonable steps to comply with Sections 4, 5, and 7 of that Act.

(b) PROHIBITION AGAINST PREDATORY AND ABUSIVE USE OF ALGORITHMIC PERSONALIZATION.—

(1) OFFENSE.—

(A) In General.— Chapter 47 of title 18, United States Code, is amended by adding at the end the following new section:

"§ 1041. FRAUD IN CONNECTION WITH ALGORITHMIC PERSONALIZED CONTENT

(a) IN GENERAL.—Whoever, in or affecting interstate or foreign commerce, knowingly—

(1) Transmits, either directly or indirectly, and in return for anything of value, materially false or misleading information to an interactive computer service, with the intent that the false or misleading information will affect how any content will be presented to any user or users by the interactive computer service's algorithmic personalization processes;

(2) falsifies the identity of the user submitting content to an interactive service provider, and, in return for anything of value, intentionally initiates the submission of content, directly or indirectly, to the

[312] *Id.* § 4(c).

[313] *Id.* § 4(e).

interactive service provider, with the intent that the information will affect how any content will be presented to any user or users by the interactive computer service's algorithmic personalization processes;

(3) accesses any protected computer or user account on an interactive service without authorization and, in return for anything of value, intentionally initiates the submission of information to an interactive service provider, with the intent that the information will affect how any content will be presented to any user or users by the interactive computer service's algorithmic personalization processes;

(4) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol Addresses, and, in return for anything of value, intentionally initiates the submission of content, directly or indirectly, to the interactive service provider, with the intent that the information will affect how any content will be presented to any user or users by the interactive computer service's algorithmic personalization processes; or conspires to do so, shall be punished as provided in subsection (b).

(5) Materially.—For purposes of paragraph (1), the term "materially" includes alteration or concealment of information in the visible or invisible content provided by the information content provider that would impair the ability of the interactive computer service (a) to accurately apply its algorithmic personalization process to determine the order, relevance, prominence, prioritization, or customization of the presentation of content, products, search results, services, or other information presented to a user; or (b) to accurately display content in a non-algorithmic way, not based on algorithmic personalization.

(6) Affirmative defense.—If shall be an affirmative defense to the crimes in paragraph (a) if it was unreasonable for the accused to intend that the information would affect the display of content, given how the interactive computer service's algorithmic personalization processes work.

(b) PENALTIES.—The punishment for an offense in subsection (a) is—

(1) a fine under this title, imprisonment for not more than 5 years, or both, if—

(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

(B) the defendant has previously been convicted under this section, section 1037, or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

(2) a fine under this title, imprisonment for not more than 3 years, or both, if—

(A) the number of users the content was displayed to exceeded 100,000 users during any 24-hour period, 1,000,000 in any 30-day period, or 100,000,000 during any 1-year period;

(B) the offense caused a loss to one or more persons aggregating $5,000 or more in value during any 1-year period; or

(C) the offense was undertaken by the defendant in concert with three or more persons with respect to whom the defendant occupied a position of organizer or leader; and

(3) a fine under this title or imprisonment for not more than 1 year, or both, in any case.

SECTION 7. QUALIFIED RESEARCH PROJECTS, QUALIFIED RESEARCHERS, AND QUALIFIED DATA AND INFORMATION.[314]

SECTION 8. ALGORITHM RESEARCH REPORTING TO CONGRESS.[315]

SECTION 9. ENFORCEMENT

(a) ENFORCEMENT BY THE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—An interactive service provider's failure to comply with Section 4 or Section 5 of this Act, a commercial information content provider's violation of Section 6(b), or a qualified researcher's failure to comply with subsection (a) or (b) of Section 10, shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF THE COMMISSION.—[316]

(3) Regulations.—[317]

(4) Attorney's Fees and Other Costs.—[318]

(b) ENFORCEMENT BY STATES.—

(1) AUTHORIZATION.—Subject to paragraph (2), in any case in which the attorney general of a State has reason to believe that an interest of the residents of the State has been or is adversely affected by the engagement of any person in an act or practice that violates this Act or a regulation promulgated under this Act, the attorney general of the State may, as parens patriae, bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

[314] *Id.* § 3 (prescribing process for NSF and FTC to create program to review research applications for approval as qualified research projects), § 4 (providing immunity to qualified researchers that properly access and use data under the Act, and preserving platform ability to protect life and physical safety, and ability to respond to security incidents, identity theft, fraud, harassment, deceptive or illegal activities, preserve system integrity, and report wrongdoers).

[315] *Id.* § 6 (establishing a requirement for the NSF and Commission to submit annual reports to Congress identifying qualified researchers, the interactive computer services involved, categories of data provided, and recommendations to increase transparency).

[316] *Id.* § 7(a)(2).

[317] *Id.* § 7(b).

[318] *Id.* § 7(c).

(A) enjoin that act or practice;

(B) enforce compliance with this Act or the regulation;

(C) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of the State; or

(D) obtain such other relief as the court may consider to be appropriate.

(2) RIGHTS OF THE COMMISSION.—

(A) NOTICE TO THE COMMISSION.—[319]

(B) INTERVENTION BY THE COMMISSION.—The Commission may—

(i) intervene in any civil action brought by the attorney general of a State under paragraph (1); and

(ii) upon intervening—

(I) be heard on all matters arising in the civil action; and

(II) file petitions for appeal of a decision in the civil action.

(3) INVESTIGATORY POWERS.—Nothing in this subsection may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.[320]

(4) ACTION BY THE COMMISSION.—If the Commission institutes a civil action . . . the attorney general of a State may not, during the pendency of the action, bring a civil action . . .[321]

(5) VENUE; SERVICE OF PROCESS.—[322]

(c) ENFORCEMENT BY THE DEPARTMENT OF JUSTICE.—[323]

(1) IN GENERAL.—The Attorney General may bring a civil action to enforce sections 4 or 5 in an appropriate district court of the United States.

(2) COORDINATION WITH THE COMMISSION.—The Attorney General shall, when reasonable and appropriate, consult and coordinate with the Commission on a civil action brought under paragraph (1).

(3) RELIEF.—In any civil action brought under paragraph (1), the court may impose injunctive relief, declaratory relief, damages, civil penalties, restitution, and any other relief the court deems appropriate.

(d) ENFORCEMENT BY INDIVIDUALS.—[324]

(1) IN GENERAL.—Any individual alleging a violation of section 4 or 5, or a regulation promulgated thereunder, may bring a civil action in any court of competent jurisdiction, State or Federal.

(2) RELIEF.—In a civil action brought under paragraph (1) in which the plaintiff prevails, the court may award—

(A) an amount equal to $2,500 or actual damages, whichever is greater;

(B) punitive damages;

[319] *See* TCPA, 47 U.S.C. § 227(e)(6)(B) (notice of intervention by FTC to state attorney general); *see* H.R. 4624 § 8(b)(2)(A) (2023).

[320] *See* TCPA, 47 U.S.C. § 227(e)(6)(D) (TCPA preserves attorney general investigatory and other powers); *see* H.R. 4624 § 8(b)(3).

[321] *See* H.R. 4624 § 8(b)(4).

[322] *See id.* § 8(b)(5).

[323] *See id.* § 8(c).

[324] *See id.* § 8(d).

(C) reasonable attorney's fees and litigation costs; and
(D) any other relief, including injunctive or declaratory relief, that the court determines appropriate.

SECTION 10. OBLIGATIONS AND IMMUNITY FOR QUALIFIED RESEARCHERS.[325]

SECTION 11. ESTABLISHING A SAFE HARBOR FOR RESEARCH ON SOCIAL MEDIA PLATFORMS.[326]

SECTION 12. RULEMAKING AUTHORITY.[327]

SECTION 13. AUTHORIZATION OF APPROPRIATIONS.[328]

SECTION 14. SEVERABILITY.[329]

h. Considering possible objections to the American Algorithmic Choice and Transparency Act.

i. Objections to creating a private right of action would likely fail if Congress acts based on the nuisance and societal harms of algorithmically amplified content.

One possible attack on the ACT-Act would be that consumers lack standing, because they have not suffered a particularized injury, such that cases like *Spokeo, Inc., v. Robbins,*[330] bar monetary damages. But this is unlikely to succeed, by *Spokeo'*s language itself, and given precedent since *Spokeo*. First, *Spokeo* notes that a "concrete," but not necessarily "tangible," injury must exist—and "history and the judgment of Congress play important roles" in determining if a concrete injury exists.[331] The Supreme Court says "Congress is well positioned to identify intangible harms that meet minimum Article III requirements . . . [and] Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.'"[332]

[325] S. 1876 § 5 (setting limits on how qualified researchers may use qualified data, protections for personal information, and civil and criminal liability for violation of privacy and cybersecurity safeguards by qualified researchers).
[326] *Id*. § 8 (generally barring civil claims against a person collecting information as part of newsgathering or research on a platform, so long as the person is conducting digital investigation on matters of public concern and takes reasonable measures to protect the privacy of users).
[327] *Id*. § 9 (prescribing how FTC, in consultation with the NSF, may issue regulations to govern how the FTC may make "data, metrics, or other information that the [FTC] determines will facilitate independent research" available to qualified researchers, and requiring the FTC to issue regulations on advertising transparency, algorithm transparency, and content moderation transparency).
[328] *Id*. § 10.
[329] *Id*. § 11.
[330] *Spokeo, Inc., v. Robins,* 578 U.S. 330, 330 (2016).
[331] *Id*. at 341.
[332] *Id*. (citing *Vermont Agency of Natural Resources v. United States ex rel. Stevens,* 529 U.S. 765, 775-777 (2000)).

Congress can thus create private rights of action for nuisance,[333] or create a statutory cause of action to remedy the sharing of private information with third parties by way of recommendation algorithms—even if that sharing is merely an "intangible harm."[334]

Here, the act of collecting and using the massed sensitive and private information of users, without their consent, to send unsolicited content to them and connect them to third parties—invokes both nuisance and invasion of privacy issues. If the internet platform collects information about user behavior and does nothing with it—then perhaps users will be unaffected. But flooding search results, or social media streams and recommendation engines, with unsolicited content based on linking that personal information to third party content providers and advertisers—and pushing users into contact with ever more radical and unwanted third parties—is clearly a proper basis for regulation and creation of a monetary private right of action.

ii. If algorithms are commercial speech, requiring internet platforms to provide an option to opt-out of personalization algorithms, should pass constitutional muster.

Even assuming algorithms are commercial speech, the First Amendment protects commercial speech to a lesser extent than noncommercial speech.[335] In *Central Hudson,* the Supreme Court provided an intermediate scrutiny review of restrictions on commercial speech under the First Amendment: (1) the commercial speech must concern lawful activity and not be misleading; (2) the governmental interest in regulating the speech must be substantial; (3) the regulation must directly advance the government's asserted interest; and, (4) the restriction must be no more extensive than necessary to serve the interest.[336]

Since *Central Hudson,* the Supreme Court in *Sorrell* struck down a Vermont statute that permitted some purchase of pharmacy records that identify the prescribing doctors—but specifically prohibited purchases of those same records for the purpose of marketing, and it prohibited pharmacies, health insurers, and pharmaceutical manufacturers from using the information for marketing.[337] The *Central Hudson* Court applied heightened scrutiny, striking down the measures, finding that the government regulation was content-based and impermissibly specifically restricted marketing speech, but favored other types of speech.[338]

[333] *Melito v. Experian Mktg. Solutions, Inc*., 923 F.3d 85, 88 (2d Cir. 2019) (one or two text messages is sufficient nuisance-based harm for standing under the TCPA: "The principal question we are tasked with deciding is whether Plaintiffs' receipt of the unsolicited text messages, sans any other injury, is sufficient to demonstrate injury-in-fact. We hold that it is. First, the nuisance and privacy invasion attendant on spam texts are the very harms with which Congress was concerned when enacting the TCPA. Second, history confirms that causes of action to remedy such injuries were traditionally regarded as providing bases for lawsuits in English or American courts. Plaintiffs were therefore not required to demonstrate any additional harm. Having concluded that Plaintiffs have satisfied Article III's standing requirement, we dismiss Experian's appeal for lack of appellate jurisdiction and affirm the judgment of the district court with respect to Bowes's appeal.").

[334] *In re Horizon Healthcare Servs. Data Breach Litig*., 846 F.3d 625, 636-38 (3rd Cir. 2017).

[335] *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.,* 425 U.S. 748, 770-73 (1976).

[336] *Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 566 (1980).

[337] *Sorrell v. IMS Health Inc*., 564 U.S. 552, 559 (2011).

[338] *Id.* at 566.

On the other hand, most internet service profits derive from advertising: the activities and data of users are the commodities internet platforms sell to make profit.[339] Platform algorithms today are almost certainly, if speech, then "commercial speech." The U.S. Court of Appeals for the District of Columbia Circuit in *Trans Union Corp. v. FTC* rejected TransUnion's claim that its "target marketing lists" should have been reviewed for strict scrutiny rather than intermediate scrutiny, as commercial speech.[340] The court found that the marketing lists, as commercial speech, were not matters of public concern—instead they "interest only Trans Union and its . . . customers" to whom Trans Union sells the lists of consumer data.[341] The court further rejected Trans Union's argument that Congress should have adopted an "opt-out" scheme for consumers, rather than the more speech-restrictive "opt-in" to allow Trans Union to share data with third parties.[342]

Similarly, the consumer personal data Facebook, Twitter, TikTok, Google, and other internet services collect for their advertising business is often not publicly available information but is *Carpenter*-type "mosaic theory" data like location information, IP address information, emails, online behavior, search queries, and other data that most individuals presume is not openly available to the public. The two sides that engage in commercial transactions with that data are internet platforms like Google and Facebook—and advertisers.

Content-neutral regulations requiring internet companies to provide an "opt-out," should easily pass intermediate scrutiny. An opt-out option will not suppress the "commercial speech" of the algorithm—consumers can turn it back on. Nor does it suppress the speech of information content providers—the proposed statute instead merely requires that platforms provide a non-algorithmic way to view the same content.

iii. The requirement to make factual, uncontroversial disclosures, to avoid deception of internet platform users, will likewise survive First Amendment scrutiny.

Likewise, the Supreme Court applies lower scrutiny to compelled commercial disclosure requirements to consumers, under cases like *Zauderer v. Office of Disciplinary Counsel.*[343] The Court found that the service provider's First Amendment rights were reasonably protected because the disclosure requirement was "reasonably related" to the government's interest "in preventing deception of consumers." Disclosure requirements are generally considered content based, but commercial disclosures are often upheld if the compelled disclosure is "factual and uncontroversial,"[344] related to the services the speaker provides,[345] and relate to the government interest in preventing deception—though lower courts sometimes apply *Zauderer* to other

[339] Erin Bernstein & Theresa J. Lee, *Where the Consumer is the Commodity: The Difficulty with the Current Definition of Commercial Speech,* 2013 MICH. ST. L. REV. 39, 62-63 (2013).
[340] *Trans Union Corp. v. FTC*, 267 F.3d 1138, 1140-41 (D.C. Cir. 2001).
[341] *Id.* at 1140.
[342] *Id.* at 1143.
[343] *Zauderer v. Office of Disciplinary Counsel,* 471 U.S. 626, 651 (1985).
[344] *Zauderer*, 471 U.S. at 651; *see also, e.g., Nat'l Inst. of Family & Life Advocates v. Becerra,* 138 S. Ct. 2361, 2372 (2018) [hereinafter NIFLA]; *Am. Meat Inst. v. United States Dep't of Agric.*, 760 F.3d 18, 21-22 (D.C. Cir. 2014) (en banc) [hereinafter AMI]; *N.Y. State Rest. Ass'n v. N.Y.C. Bd. of Health*, 556 F.3d 114, 134 (2d Cir. 2009) [hereinafter NYSRA].
[345] *See NIFLA,* 138 S. Ct. at 2372.

situations.[346] Numerous similar disclosure requirements already exist in federal law, from disclosing bioengineered food,[347] to direct to consumer advertisements for prescription drugs and drug side effects,[348] to energy efficiency labels for appliances.[349]

So too here. The disclosure of what data is collected, and how algorithms work, is factual and uncontroversial.[350] The disclosure is unquestionably related to the services platforms provide. Finally, the United States' interest is both directed at combatting deception of consumers,[351] and preventing consumers from being misled[352] about the nature of the underlying commercial relationship between the user, the online platform, and advertisers. And the United States' interest in preventing deception, radicalization, self-harm, violence, and other ills, to consumers, is reasonably related[353] to requiring platforms to disclose how their commercially-beneficial algorithms work to gather personal data, work to keep users on the site, and deliver the ongoing collection of data to the advertisers that pay the platforms.[354] The "notice" and "choice" proposals are so standard, in fact, that little stands in the way of Congress acting now.

IV. **Conclusion**

It's a common theme in some of the best science-fiction movies that the protagonists are confronted by a super-intelligent artificial intelligence threatening the world—or the protagonists' world—and the heroes must find a way to "turn off" the computer or robot to survive. HAL 9000, in Stanley Kubrick's classic "2001," had to be "turned off" with great difficulty by Dave, after HAL killed the other members of the spaceship Discovery One.[355] In the 1980's cult-classic "The Terminator," a robot from the future played by Arnold Schwarzenegger went on a killing rampage until the hero Sarah Connor could "terminate" the robot by smashing its computer brains in a hydraulic press.[356] And in "The Matrix" series, humankind is enslaved in a virtual reality until the hero Neo, played by Keanu Reeves, escapes from the computer simulation and "disconnects" humans from the machines.[357]

The common thread here, of course, is that these movies would have been a lot less fun had Congress mandated that all supercomputers have an easily accessible "off switch." That "kill switch" is common in American legislation—it's the "consent" and "opt-out" provisions of the TCPA and CAN-SPAM Act, and in so many other laws Americans encounter every day. Had any

[346] *E.g., AMI*, 760 F.3d at 22; *NYSRA*, 556 F.3d at 133.

[347] 7 U.S.C. § 1639b(a); 7 C.F.R. § 66.3.

[348] 21 U.S.C. § 352(n).

[349] 42 U.S.C. § 6294; 16 C.F.R. § 305.

[350] *Milavetz, Gallop & Milavetz, P.A. v. United States*, 559 U.S. 229, 250 (2010) ("[T]he disclosures entail only an accurate statement identifying the advertiser's legal status and the character of the assistance provided[.]").

[351] *Zauderer*, 471 U.S. at 651.

[352] *Milavetz,* 559 U.S. at 250.

[353] *See Zauderer*, 471 U.S. at 651.

[354] *See AMI*, 760 F.3d at 26; *see also, Conn. Bar Ass'n v. United States*, 620 F.3d 81, 97 (2d Cir. 2010) ("[O]nce the government demonstrated that ignorance, confusion, and deception infected the bankruptcy process in the late 1990s, the persistence of such problems was sufficiently evident that no subsequent surveys were required to support congressional action in 2005 mandating information disclosure to consumer debtors.").

[355] 2001 (MGM, Stanley Kubrick Productions Apr. 2, 1968).

[356] THE TERMINATOR (Cinema '84 Oct. 26, 1984).

[357] THE MATRIX (Warner Bros. Mar. 24, 1999).

of the heroes of these movies been fully apprised of the great dangers caused by the artificial intelligence algorithms—just as Americans are warned about the health dangers of cigarettes and alcohol—they might not have gotten themselves in such a pickle with killer robots.

If American consumers are provided notice and choice—if researchers and Congress gain deep understanding of how algorithms affect crowd behavior online—if we accomplish these basics, then the freedom of individual choice, with this much needed knowledge, can be well-informed. With enforcement from the FTC, violators can be held to account. With a private right of action and the types of effective "bounty" rights of action that have worked in other contexts, we can hold information content providers to account when they violate the transparent algorithmic explanations we will require of platforms.

We have seen this threat growing for almost fifteen years. We have faced world disorder and insurrection at home stoked by algorithms. The threat is existential. Congress must act now.