Testimony of Laurel Lehman
Policy Analyst, Advocacy
Consumer Reports

Before the
United States House of Representatives Committee on Energy & Commerce
Subcommittee on Consumer Protection and Commerce

Hearing on
"Holding Big Tech Accountable: Legislation To Protect Online Users"

March 1, 2022

Thank you Chair Schakowsky, Ranking Member Bilirakis, and Members of the Subcommittee, for inviting Consumer Reports (CR) to testify on the crucial matter of tech accountability and protecting consumers online. CR was founded in 1936 and at a time of rapidly proliferating new technologies. A new media landscape was riddled with unfettered advertising claims that paltry patchwork regulation did little to address. As a result, consumers were left with precious few ways to gauge the value, quality, or authenticity of goods and services.

For 86 years, consumers have turned to CR for answers to questions such as, "Is this product safe? Is it worth my time or money? What risks might it pose to me or my family? How does it perform day-by-day? How does that change over time? How will it hold up under stress?"

Consumers today grapple with the same questions, but about their online experiences. Today's hearing, focused on ways to protect consumers online, is the digital version of the very same challenges that have driven CR's mission all along.

CR has surveyed consumers extensively on these topics in the last year, to better understand their concerns as we work towards workable solutions. Consumers face a range of issues online: in an August 2021 nationally-representative Consumer Reports survey, 94% of Americans said they had ever had at least one social media account. Among those, 84% had ever adjusted their social media settings to limit or filter content in some way (with 39% electing to turn off targeted ads); 59% said that they had read news on social media that they initially believed to be true but later learned was made up; and 37% percent had, at some point, wanted to change their privacy settings on a social media platform but didn't know how.[1]

Consumer concerns in the digital marketplace are not limited to social media, and expand to e-commerce. While nearly two-thirds of Americans told us in CR's November 2021 nationally-representative survey that they often or always read online reviews to help them decide what to buy, nearly eight out of ten (79%) of people who read online reviews before deciding what to buy say they have ever read a review that they thought was fake.[2] And, in CR's September 2021 nationally-representative survey, consumers were overwhelmingly opposed to online retailers using personalized pricing: seven in ten Americans oppose this practice, with 49% of Americans saying they "strongly oppose it."[3]

Finally, even as artificial intelligence (AI) proliferates rapidly across consumer sectors, more than three-quarters (76%) say they would be uncomfortable (very uncomfortable; 46%,

[1] August 2021 Consumer Reports nationally representative Social Media Survey of 2,263 US adults.

[2] November 2021 Consumer Reports nationally representative American Experiences Survey of 2,057 US adults.

[3] September 2021 Consumer Reports nationally representative American Experiences Survey of 2,341 US adults. Personalized pricing was described in this way: "Online retailers are in the practice of selling the same goods and services at different prices, depending on things like your income, home address, age, credit rating, browsing history and other personal information. This can result in someone being charged more or less than the standard retail price, depending on the algorithm used."

somewhat uncomfortable; 30%) allowing AI to screen a video by grading responses and facial movements of them answering preselected questions during the job interview process. Furthermore, 62% say they would be uncomfortable allowing banks to use AI to make credit decisions to determine if they would qualify for a personal loan, and 52% would be uncomfortable using AI in hospital systems to help make diagnoses and a treatment plan.[4]

The digital marketplace is as varied in potential solutions as it is in its issues. Just as no singular recall, regulation, safety standard, or warning label can unilaterally keep consumers safe offline, the variety of challenges consumers face online also require comprehensive engagement with a full toolbox of evidence-based legislative, regulatory, and standards-driven solutions. Current law governing the online information ecosystem both fails to provide sufficient incentive for tech platforms to take responsibility for the harms that their systems compound and accelerate, and fails in parallel to equip regulators, researchers, and the public with the tools and context necessary to understand and help mitigate these harms.

In short, consumers deserve a safe, just, transparent information and e-commerce ecosystem that they can trust. Congress can—and must—work to pass legislation that makes it possible.

I. Transparency: Baseline Initiatives

CR has long advocated for transparency across the board for consumers, and the digital marketplace is no exception. When consumers are buying cars, appliances, or new electronics they ask, "What kind of performance can I expect? How does it perform over time and under stress? What safety standards does the manufacturer adhere to?" And consumers can get some answers from mandated testing, safety ratings and standards, and disclosures—like window stickers detailing a car's mileage—and still other answers come from research and testing by independent parties like CR. Yet despite more and more critical components of our lives taking place online—particularly in the wake of COVID-19—consumers online have nowhere near such insight for digital products behind ever-growing screen-time: the internet has no crash-test disclosures.

That is why CR was proud to support the requirement that internet service providers (ISPs) display a "consumer broadband label" (or broadband nutrition label) detailing the price,

[4] September 2021 Consumer Reports nationally representative American Experiences Survey of 2,341 US adults. AI was described in this way: "Artificial intelligence (AI) is a branch of computer science concerned with building smart machines capable of performing tasks such as problem-solving and decision making that would otherwise require human intelligence. Artificial intelligence is all around us and playing an active role in our daily lives. Every time we open our Facebook newsfeed, do a Google search, get a product recommendation from Amazon or book a trip online from Travelocity, AI is working in the background to learn from and adapt to data input in real time, and refine the content that is delivered." For each of these situations, 7-8% of respondents said they were "unsure" how they would view it.

performance, and speed of internet access for consumers to help them make better decisions about broadband service. It represents a step in the right direction, but much more needs to be done in the online space.

Auto and product manufacturers are expected to conduct safety testing, and CR can test cars and appliances for performance under stress to see how manufacturer claims line up with their advertising. Digital product manufacturers, however, have no such obligations to research, mitigate, or disclose risks or dangers in the manufacturing of their information display and content moderation pipelines. They need not publish clear community guidelines or terms of service, or report on how effective their enforcement of such guidelines may be (indeed—CR published a guide on various' platforms misinformation policies early in the COVID-19 pandemic because so much consumer confusion persisted[5]) and they make no guarantees that they are appropriately staffing and equipping the teams dedicated to keeping consumers safe from harassment, spam, hate speech, and misinformation.

In August 2021, the lead researcher for NYU Cybersecurity for Democracy, Laura Edelson, was running the program's Ad Observatory—a crowdsourced effort where consumers shared political ads they had been shown, in an effort to understand how political ads were targeted. Only hours after informing Facebook that she and her team were studying how disinformation about the Jan. 6 attack on the U.S. Capitol had proliferated on the platform, Facebook disabled their accounts.[6] And last summer reporting on Facebook's internal chafing at the narratives that CrowdTangle—the data analytics tool they had acquired that offered some insight into news and misinformation spread across their platforms—had made possible before Meta disbanded the team running the tool.[7] Google notoriously fired AI ethicist Timnit Gebru—and shortly after, her AI ethics colleague Margaret Mitchell as well—after their team sought to publish on the risks of AI systems Google was developing.[8] Time and time again, platforms have shown that when researchers attempt to set-up test tracks to better understand the algorithmic systems driving the public's online information ecosystem—tech giants will move to shut them down.

[5] CR, "On Social Media, Only Some Lies Are Against the Rules" (Aug. 13, 2020) (online at: https://www.consumerreports.org/social-media/social-media-misinformation-policies/)
[6] AP, "Facebook shuts out NYU academics' research on political ads" (Aug. 4, 2021) (online at: https://apnews.com/article/technology-business-5d3021ed9f193bf249c3af158b128d18)
[7] New York Times, "Inside Facebook's Data Wars" (Jul. 14, 2021) (online at: https://www.nytimes.com/2021/07/14/technology/facebook-data.html)
[8] Washington Post, "Google hired Timnit Gebru to be an outspoken critic of unethical AI. Then she was fired for it." (Dec. 23, 2020) (online at: https://www.washingtonpost.com/technology/2020/12/23/google-timnit-gebru-ai-ethics/); *see also:* BBC, "Margaret Mitchell: Google fires AI ethics founder" (Feb. 20, 2021) (online at: https://www.bbc.com/news/technology-56135817)

Requests for transparency along these lines are not new,[9] and—Meta's recent market cap drop notwithstanding—the largest platforms do not lack the resources to make such transparency possible. Yet consumers—and those who would seek to protect them—remain left operating in the dark. These companies claim to be proud of how effectively they protect consumers, releasing reports packed with statistics that sound great on paper—yet fail to convey the whole picture.[10]At the end of the day, if these companies were truly proud of how effectively they protect consumers in their product design and moderation practices—we would expect them to welcome independent researchers verifying their claims, not shut down the test track.

What's more, transparency propositions are thoroughly bipartisan. The reintroduced bipartisan Platform Accountability and Consumer Transparency (PACT) Act, which would modify Section 230, details an incredible amount of content moderation process transparency, and the bipartisan Platform Accountability and Transparency Act (PATA) is designed to offer researchers and the public access to platform data.[11] House Energy and Commerce Ranking Member McMorris Rodgers' Big Tech Accountability Platform Memo last year sought to, "Require disclosures regarding how Big Tech develops its content policies and require regular disclosures about content policy enforcement, including the types of content taken down and why, and clearly understood appeals processes," and Democratic proposals have ranged from those before the Subcommittee today, to last year's Algorithmic Justice and Online Platform Transparency Act**.**[12]

Furthermore, different stakeholders in the online information ecosystem are best served by different kinds of transparency. While troves of granular details can overwhelm everyday consumers — and can sometimes place the onus for a platform's responsibility on consumers unlikely to make use of such knowledge—at scale, granular data can help researchers and agencies with vested public consumer interests understand the extent of broader societal consequences of shifts in online platform information ecosystems. For ordinary users, access to ad libraries may prove useful references to better understand trends in the brands they buy from.

However, across urgently needed increased dimensions of transparency—though most especially when it comes to independent researcher access to platform data—balancing the public interest with legitimate consumer privacy concerns must be paramount. In this vein, CR urges researcher access provisions that start with a baseline standard for de-identification—at

[9] The Atlantic, "Rage Against the Algorithms" (Oct. 3, 2013) (online at: https://www.theatlantic.com/technology/archive/2013/10/rage-against-the-algorithms/280255/)

[10] Wired, "Facebook Uses Deceptive Math to Hide Its Hate Speech Problem" (Oct. 15, 2021) (online at: https://www.wired.com/story/facebooks-deceptive-math-when-it-comes-to-hate-speech/)

[11] The Platform Accountability and Consumer Transparency (PACT) Act, S. 797, 117th Cong., (2021); The Platform Accountability and Transparency Act (PATA), S. XX, 117th Cong., (2021)

[12] Republican Leader McMorris Rodgers to Energy and Commerce Committee Republican Members, "Memo Re: Big Tech Accountability Platform" (Jan. 26, 2021) (online at: https://republicans-energycommerce.house.gov/wp-content/uploads/2021/01/Big-Tech-Accountability-Platform-Memo.pdf); Algorithmic Justice and Online Platform Transparency Act, H.R. 3611, 117th Cong., (2021)

least for all private content, and likely too for some public content—as defined by three prongs in the FTC's 2012 Privacy report: achieving a reasonable level of justified confidence that the data cannot reasonably be used to infer information about a particular consumer or device; a commitment not to attempt to re-identify, and contractual obligations preventing any shared entities (if any) from attempting to reidentify.[13]

Finally, in order to future-proof transparency mechanisms in the digital ecosystem, legislation driving these efforts must build in the level of flexibility and nuance required to encompass the most relevant expectations across a variety of platform purposes, sizes, and structures, and be adaptable to changing technologies. Regulators should be explicitly given rulemaking authority, which would offer more nimble, adaptable, and industry-specific rules going forward in perpetuity than would fixed statutory requirements alone.

Keeping such distinctions in mind, we urge Congress to consider a variety of initiatives that might improve platform transparency, and offer three pillars to consider in doing so: pipelines, processes, and personnel.

Pipelines

Online platforms are made up of information pipelines: the pieces of virtual infrastructure that direct both how content is ultimately delivered to users (e.g. ads and algorithmic recommendations) and how content is siphoned out of the ecosystem (e.g. automated removal or downranking of content with particular qualities). Pipeline transparency should offer context around factors affecting the inputs entering the information ecosystem (display pipelines) and factors affecting what is taken out of the information ecosystem (moderation pipelines).

Display Pipelines

Transparency into display pipelines should uncover what kinds of factors affect and influence what users see — both ads and algorithmically sorted and recommended content. Display pipeline transparency should provide insight into how dollars, engagement, targeting, and display rankings affect and influence what consumers see, and affect various groups of consumers—especially minors, vulnerable populations, or marginalized communities—differently. The NYU Ad Observatory, which used to, "identify trends in how ads are targeted to specific audiences and what messages are being used, who is funding each ad and how much they are spending to disseminate them" before Meta cut them off, is an excellent example of an

[13] FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012) (online at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, pg. 21)

independent attempt at display pipeline transparency.[14] The information gathered helped inform consumers, advertisers, and policymakers — which, contrary to Meta's privacy claims, was likely a portion of why they were shut down.

Components of comprehensive display pipeline transparency might include publicly accessible ad libraries alongside reach and engagement numbers, datasheets for data sets[15], risk and impact assessments for display algorithms, transparency reporting with commonly defined metrics, and—in line with deidentification baselines laid out above, alongside other aggregation—substantial access to datasets for both independent researchers and for the FTC.

Moderation pipelines

Transparency for moderation pipelines should offer insight into how content is flagged for moderation in the first place— whether by reports from users or other entities, or by machine-learning driven automation. Such transparency should aim to answer questions such as: What datasets are those machine learning models built upon? Are they representative? Are they accurate? How often are they updated? Which content is flagged, how is it reviewed, and how is content prioritized for review? Does such review disproportionately affect different groups of consumers, or different types of content?

Potential mechanisms of transparency for moderation pipelines include risk assessments and datasheets for the algorithms used to proactively flag content for removal, transparency reporting with commonly defined metrics, and—in line with deidentification baselines laid out above, alongside other aggregation—substantial access to datasets for both independent researchers and for the FTC.

Processes

Process transparency should encompass transparency across a platform's policies and the realities of how those policies are enforced. Consumers use online platforms more than ever before for education, commerce, work, social connection, and deserve to have the specific rules of the road plainly stated and consistently enforced. They should also have a clear understanding of what to expect throughout the policy enforcement process, and where to turn for review if they believe the platforms have erred in their enforcement. Consumers also deserve clear specificity from these policies in order to understand what values they can expect the platforms they use to uphold, as overly vague platform policies lend themselves to inconsistent and unpredictable enforcement.

[14] The George Washington University's Institute for Data, Democracy & Politics, "Update: NYU Ad Observatory" (Aug. 11, 2021) (online at: https://iddp.gwu.edu/nyu-ad-observatory)

[15] CACM, Gebru et. al, "Datasheets for Datasets" (Dec. 2021) (arXiv:1803.09010) (online at: https://arxiv.org/abs/1803.09010)

Such clarity could be a key step forward in improving consumer experiences—and holding platforms more publicly accountable for their enforcement—as the largest platforms have repeatedly shown failures both to enforce their guidelines against the powerful—politicians, influencers, and advertisers—and to over-enforce them against marginalized communities. In many cases the largest platforms have over-moderated or removed content where activists talk *about* the hate and harassment they receive, or that use dialects and vernacular of marginalized communities, even as those same platforms dither and delay enforcing platform policies when the uploading users are advertisers, influencers, politicians, or otherwise already in positions of power.[16] Meanwhile, researchers and regulators need more to understand the far-reaching effects that such enforcement—and failures thereof or inconsistencies therein—can have on the online information and e-commerce ecosystem.

Publishing acceptable terms of use, community guideline, and enforcement policies; informing consumers of content removals and successful appeals, and regular, thorough transparency reports encompassing content moderation practices and metrics, granting researcher access to evaluate platform processes, and perhaps exploring timeliness requirements, with respect to reported content—might all prove steps toward a fairer online ecosystem for consumers to engage with.

Personnel

And finally, ideally, CR urges policymakers to consider two kinds of personnel transparency that would lead to improved online information ecosystems for consumers. First, transparency that would highlight whether a platform is appropriately staffed and resourced to enforce its own terms of service across the markets where it operates. This would particularly help to mitigate crises like platforms' disproportionate failures to moderate with the appropriate linguistic and cultural context in non-English-speaking markets. Domestically, failures bear consequences like the disproportionate spread of Spanish-language misinformation in the US, particularly around COVID-19 and vaccine information[17]— made even more concerning

[16] USA Today, "Facebook apologizes to black activist who was censored for calling out racism" (Aug. 3, 2017) (online at: https://www.usatoday.com/story/tech/2017/08/03/facebook-ijeoma-oluo-hate-speech/537682001/; *see also:* The Verge, "Facebook says it 'mistakenly' suspended hundreds of activists' accounts" (Sep. 24, 2020) (online at: https://www.theverge.com/2020/9/24/21454554/facebook-acitivists-suspended-accounts-coastal-gaslink-pipeline); *see also:* Washington Post, "YouTube's arbitrary standards: Stars keep making money even after breaking the rules" (Aug. 9, 2019) (online at: https://www.washingtonpost.com/technology/2019/08/09/youtubes-arbitrary-standards-stars-keep-making-money-even-after-breaking-rules/); *see also*: Sexuality and Culture, "Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online" (Nov. 6, 2020) (online at: https://link.springer.com/article/10.1007/s12119-020-09790-w); *see also:* Association for Computational Linguistics, In Proceedings of the Third Workshop on Abusive Language Online, pgs. 25–35. Davidson et. al, "Racial Bias in Hate Speech and Abusive Language Detection Datasets." (Aug. 1, 2019) (online at: https://aclanthology.org/W19-3504.pdf)

[17] Washington Post, "Misinformation online is bad in English. But it's far worse in Spanish" (Oct. 28, 2021) (online at: https://www.washingtonpost.com/outlook/2021/10/28/misinformation-spanish-facebook-social-media/); *see also:*

considering that, according to a nationally-representative CR survey, 54% of Hispanic Americans reported that they regularly get news from social media — significantly higher than any other demographic surveyed.[18] Meanwhile, as just one example, Facebook's own oversight board recommended that it engage an independent entity to audit whether its content moderation and automation across Arabic and Hebrew are applied without bias.[19] Any transparency reporting and risk assessments should include detailed breakdowns of content moderation and product design staff, ensuring appropriate sensitivity to nuance across linguistic and cultural differences where platforms operate..

Second, whistleblower protections for employees and contractors would prove invaluable—as we have already seen from the likes of pathbreaking whistleblowers like Ifeoma Ozoma, Sophie Zhang, and Frances Haugen.[20] Because no matter how many transparency reports and APIs are developed, without employee context for intention and trade-offs from design, enforcement, and implementation that — crucial components of the picture will remain missing. Congress should enshrine and codify strong whistleblower protections as a part of any transparency or accountability package.

H.R. 6796, the "Digital Services Oversight and Safety Act of 2022" (DSOSA)

The DSOSA lays out an ambitious plan for a new bureau at the FTC centered on the oversight and safety of digital services and platforms. Such central and devoted resources would be key for protecting consumers online, as a depth of expertise is required to effectively combat the harms stemming from the range of technologies, platforms, business models, that make up the information ecosystem. The bill would provide a level of both staffing and funds to the bureau befitting the broad scope of digital systems.

As we lay out in our platform accountability discussion above, DSOSA makes comprehensive platform transparency a key tenet of this new bureau. It also differentiates appropriate levels of transparency for different audiences—across different audiences—for the public, for independent researchers, and for the FTC. Such differentiation empowers consumers' understanding, without putting the onus on consumer behavior alone to fix the platforms' systemic failures. Crucially, DSOSA also recognizes that this transparency is ultimately in service of driving better understanding, prevention, and mitigation of the compounded harms that

Axios, "The Spanish-language misinformation crisis" (Feb. 8, 2022) (online at:https://www.axios.com/social-media-misinformation-latinos-2c3574d4-d437-402c-8606-94c2f6332abf.html); *see also* Time, "Facebook Says It's Removing More Hate Speech Than Ever Before. But There's a Catch" (Nov. 26, 2019) (online at: https://time.com/5739688/facebook-hate-speech-languages/)

[18] August 2021 Consumer Reports nationally representative Social Media Survey of 2,263 US adults.

[19] Facebook Oversight Board, Case decision 2021-009-FB-UA (2021) (online at: https://www.oversightboard.com/decision/FB-P93JPX02)

[20] AP, "How one Facebook worker unfriended the giant social network" (Oct. 10, 2021) (online at: https://apnews.com/article/facebook-science-technology-business-congress-frances-haugen-80e92043b7211590b6be84dcc7a05b4a)

platforms drive at scale. Rather than jumping feet first into new liability standards, it requires the largest platforms to consider, account for, and have audited their assessment of risks of societal harms throughout their systems.

While we do *not* think transparency must necessarily lead to adjustments to liability standards, DSOSA's transparency offerings could go a long way toward informing conversations around the appropriate level of liability platforms should bear, and it does not pretend to be a singular replacement for other varieties of tech policy reform (be it platform responsibility, privacy, antitrust, or otherwise), but would inform and improve all other reforms in tandem.

The bill covers substantial ground across all three transparency dimensions discussed above—ranging from process-based appeals and community standards expectations, to pipeline-based ad libraries and researcher data access, to enshrining related whistleblower protections for personnel. Again, while the bill does not pretend to be a silver bullet and focuses primarily on transparency, it would also introduce some concrete changes for consumers. As we highlight in our discussion of process transparency, it would require comprehensive appeals processes. Alongside, it would require largest covered platforms to offer an option that does not rely on any of the user's personal information to display information (with a reasonable exception for information critical to the products' functionality). And without adjusting platforms' liability immunities, it requires the largest platforms to do audited risk assessments & mitigation reports across a breadth of risks to consumers, which could incentivize greater responsibility. And, where it fails to incentivize such responsibility, the bill would still empower further research to dive into the compounding harms in the interim. Finally, we appreciate that given the bill's breadth, the scale of services covered, and the nuance required throughout the sector, how much of the bill is rooted in rulemaking, which we believe allows for the appropriate level of nuance and flexibility required of platform standards.

We also look forward to continuing to discuss elements of the bill's implementation with Representative Trahan's office, other congressional staff, and colleague organizations. While we are grateful for DSOSA's privacy protections, we do we look forward to working together to strengthen such protections even further in in future iterations — definitions of "deidentify" that align more closely with the three pillars laid out in the FTC's 2012 Privacy Report: achieving a reasonable level of justified confidence that the data cannot reasonably be used to infer information about a particular consumer or device; a commitment not to attempt to re-identify, and contractual obligations preventing any shared entities (if any) from attempting to reidentify.[21] We would also be encouraged to see a broader scope of appeals in some instances. While the bill would empower users to appeal content removals or account termination, recognizing the shift

[21] FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012) (online at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, pg. 21)

beyond the take-down/leave-up binary, we might be inclined to see the scope of mandated appeals expand to some of the more moderate moderation[22] possibilities. These might include intermediate actions such as demonetization, feature suspensions, and downranking—not least because otherwise, one could envision a world where platforms pivot to downranking content and feature-limiting users nearly out of existence instead of terminating service outright, leading to even greater opacity.

II. Platform Accountability: Negligent Design & Consumer Protection Approaches

Online platforms need to take more responsibility for the design and maintenance of their digital products and services, and they should be obligated to consider values beyond shareholder value — be it consumer safety, civic well-being, or free expression. Platforms have repeatedly demonstrated themselves unwilling to take responsibility for the harms they accelerate.

In 2020, Facebook users reported a Kenosha Militia event asking attendees to bring weapons 455 times and the platform failed to act.[23] The same year, a CR investigation found Facebook's ad approvals system approved a number of ads with misleading and outrageous COVID-19 misinformation.[24] YouTube failed to ban vaccine misinformation until September 2021—despite precedent in other tech platforms having done so as early as the first quarter of 2019—more than a year before the COVID-19 pandemic even began.[25]

Investigative reports and agency investigations have repeatedly surfaced unsafe, untested, counterfeit, and even recalled products across Amazon, Facebook Marketplace, craigslist, and a variety of e-commerce platforms. Most gallingly, these often concern products with crucial safety implications, ranging from faulty carbon monoxide detectors to baby products and bike helmets that fail to meet safety standards.[26] Meanwhile, adding insult to injury, consumers bear

[22] (no pun intended)

[23] Buzzfeed News, "A Kenosha Militia Facebook Event Asking Attendees To Bring Weapons Was Reported 455 Times. Moderators Said It Didn't Violate Any Rules." (Aug. 28, 2020) (online at: https://www.buzzfeednews.com/article/ryanmac/kenosha-militia-facebook-reported-455-times-moderators)

[24] CR, "Facebook Approved Ads with Coronavirus Misinformation" (Apr. 7, 2020) (online at: https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation-a1864110559/)

[25] NPR, "YouTube Is Banning All Content That Spreads Vaccine Misinformation" (Sep. 29, 2021) (online at: https://www.npr.org/2021/09/29/1041493544/youtube-vaccine-misinformation-ban); *see also* Washington Post, "Pinterest is blocking search results about vaccines to protect users from misinformation" (Feb 21, 2019) (online at: "https://www.washingtonpost.com/business/2019/02/21/pinterest-is-blocking-all-vaccine-related-searches-all-or-nothing-approach-policing-health-misinformation/)

[26] Wall Street Journal, "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products" (Aug. 29, 2019), (online at: https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990); *see also* CR, "Bike Helmets That Don't Meet Safety Standards Are Widely Available, Consumer Reports Finds" (July 1, 2019)

the consequences for e-commerce's well-documented fake reviews problem.[27]For years, a variety of platforms failed—and continue to fail— to take seriously the spread of misinformation, hate speech, and harassment of marginalized communities, contributing to the growth of offline extremism, violence.[28]

These failures offer signposts to policymakers, indicating where legal incentives driving accountability may be worth either reinforcing or adjusting. And where online platforms clearly fail to take reasonable baseline steps to ensure their products are designed and managed responsibly, where they repeatedly choose engagement, profitability, or minimized operational costs, over harms to livelihoods, public health, and consumer well-being, there should be opportunity for recourse. Platforms should not be able to launch new products and features affecting billions of consumers without having built out the ability to reasonably enforce their own community guidelines or terms of service. Further, consumers should be able to expect that platforms have considered—and taken reasonable steps to mitigate—clearly foreseeable harms that such launches could compound or accelerate.

Section 230

While recognizing that Section 230 is not within the scope of the Consumer Protection Subcommittee, it would be irresponsible to discuss American platform accountability without some discussion. Section 230 has both protected and made possible key components of the internet's original promise *and* allowed online platforms more leeway to ignore the compounded scale of harms to consumers and society that their products and policies enable.[29]

Reforming Section 230 should be approached cautiously, and many bills that have been proposed thus far would do far more harm than good. Some proposals to modify Section 230 would seek to *disincentivize* platform moderation altogether—when it's clear that platforms need to be doing more, not less, to foster a healthier online information ecosystem and keep consumers safe. Nevertheless, we are encouraged by various component parts of the PACT Act, the Protecting Americans from Dangerous Algorithms Act, and the Justice Against Malicious

(online at: https://www.consumerreports.org/bike-helmets/bike-helmets-that-dont-meet-federal-safety-standards-are-widely-available/)

[27] TechCrunch, "Amazon deflects responsibility on fake reviews but admits 200M were blocked last year" (Jun. 16, 2021) https://techcrunch.com/2021/06/16/amazon-deflects-responsibility-on-fake-reviews-but-admits-200m-were-blocked-last-year/, *see also* CR, "Hijacked Reviews on Amazon Can Trick Shoppers" (Aug. 26, 2019) https://www.consumerreports.org/customer-reviews-ratings/hijacked-reviews-on-amazon-can-trick-shoppers/

[28] 2021 IEEE Symposium on Security and Privacy (SP,) K. Thomas *et al.*, (2021) "SoK: Hate, Harassment, and the Changing Landscape of Online Abuse," pgs. 247-267, doi: 10.1109/SP40001.2021.00028.

[29] As we discuss at length here: https://medium.com/cr-digital-lab/crs-section-230-2020-legislative-round-up-4683c309fcb3.

Algorithms Act (JAMAA), and hope to see such conversations continue in keeping with the principles that follow.[30]

As a general rule, and especially in the wake of FOSTA-SESTA,[31]eliminating Section 230 (c)(1) immunities—immunities for hosting and disseminating third-party content—by way of subject matter exemptions alone) would be irresponsible. Subject matter exemptions alone are wont to drive brunt, over-broad platform responses without addressing existing failures in platform moderation systems. However, there may be room to explore narrow subject matter exceptions when they are in combination with additional narrowing factors, such as a platform's mechanism of delivering the content. Such proposals would be along the lines introduced by the Protecting Americans from Dangerous Algorithms Act, which opened narrow civil liability for certain existing civil rights claims when platforms amplified the content in question.

Modifications that would seek to disincentivize moderation, either by removing Section 230 immunity for many subsets of content moderation, or by conditioning (c)(1) immunity on "neutral" enforcement, would run counter to consumer interests, as consumers require platforms to take more—not less—responsibility for the harms they accelerate. As discussed in the Transparency section above, process improvements and accountability mechanisms—like those found in the PACT Act, and throughout the DSOSA—would strongly benefit consumers.

JAMAA would modify Section 230 to open platforms to liability where the provider "knew or should have known" it was making a "personalized recommendation" of information, did so recklessly, and the recommendation materially contributed to injury. We are most concerned that the bill's knowledge standard would functionally the bill's knowledge standard would functionally strip Section 230 protections for any algorithmically sorted content, strongly deterring platforms from using algorithms in contexts where they may be useful. However, the JAMAA's approach furthers a useful line of conversation around Section 230, as we would be encouraged to find room to pursue further cases along the lines of negligent design (more on this below), or otherwise develop reasonable expectations on platform design. without opening the potential for so much liability that extreme over-moderation or over-monitoring of content would result.

Harmful Design

[30]Protecting Americans from Dangerous Algorithms Act, H.R. 2154, 117th Cong., (2021); Justice Against Malicious Algorithms Act, H.R. 5596, 117th Cong., (2021)

[31] Passed in 2018, this legislation combined Senate's Allow States and Victims to Fight Online Trafficking Act of 2017 (FOSTA), which combined a House bill of the same name with provisions from a Senate bill, the Stop Enabling Sex Traffickers Act (SESTA), which modified Section 230 with an exception to 230(e) to fight sex trafficking. It was a contentious measure whose full impacts are still unclear, but that has so far had clear effects on the speech of marginalized communities online. See: Fordham Law Review, "FOSTA: A Hostile Law with a Human Cost" (2019) (online at: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5598&context=flr); *see also* Out, "The Dangerous Trend of LGBTQ+ Censorship on the Internet" (Dec. 6, 2018) (online at: https://www.out.com/out-exclusives/2018/12/06/dangerous-trend-lgbtq-censorship-internet.)

Across a variety of consumer products, it is well understood that fundamentally, manufacturers and companies should bear responsibility for their design and process choices that lead to foreseeable, preventable harms to consumers using the product in its intended manner. While the way that digital products intersect with consumer data and speech complicate the premise, room remains to expand the conversation to the digital sphere.[32]

Lemmon v. Snap, Inc. is an ongoing civil lawsuit against Snap Inc, brought by the parents of two teenagers who died tragically in a car accident after reaching 123 miles per hour. The parents' suit alleges that Snapchat—having designed and offered both a "speed filter" *and* intermittent, unpredictable engagement-based rewards of "trophies, streaks, and social recognitions" that in combination could incentivize young drivers to drive at dangerously high speeds—was negligently designed. The Ninth Circuit found that Snap was "sued for the predictable consequences of designing Snapchat in such a way that it allegedly encouraged dangerous behavior." And it further found that Snap could not avail itself of Section 230 (c)(1) immunity because the suit did not rely on "information provided by another information content provider," but on Snap's, "duty to design a reasonably safe product [which] was fully independent of [its] role in monitoring or publishing third-party content."[33]

While the district court has yet to determine whether Snap is liable, that such liability is not precluded by Section 230 immunity seems to be the right result, and one legislators may wish to carefully expand. CR would be encouraged to see perhaps even a slightly broader legal avenue to pursue recourse when consumers are subject to digital products that, as-designed, or as-maintained could lead to clearly foreseeable harms—whether by way of nuanced tweaks to Section 230 or other means of imposing baseline consumer protection expectations for platforms to undertake basic best practices and reasonable steps to anticipate, prevent, and mitigate the harms their systems can accelerate, rather than apologizing for them[34].

FTC Act Section 5

Regulators also may be already able to take action against platforms that fail to take reasonable measures to protect users from the harmful acts of others on their platforms. Section 5 of the FTC Act broadly prohibits companies from committing "unfair or deceptive acts or practices" in the marketplace. Certainly if a company commits to taking certain acts to remediate bad activity, the FTC could find that failure to follow through on those commitments constitutes a deceptive practice. Moreover, in some situations, failure to enforce clear platform rules against

[32] Lawfare, "Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must be Fixed" (Aug. 14, 2019) (online at: https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed)

[33] *Lemmon v. Snap, Inc.*, No. 20-55295 (9th Cir. 2021)

[34] Wired, "Why Zuckerberg's 14-Year Apology Tour Hasn't Fixed Facebook" (Apr. 6, 2018) (online at: https://www.wired.com/story/why-zuckerberg-15-year-apology-tour-hasnt-fixed-facebook/)

bad actors could be considered deceptive, as the existence of rules in the first place may be reasonably interpreted as an implicit promise to reasonably enforce them.

The other half of the FTC's general purpose consumer protection law is "unfairness." To constitute an unfair business practice, it might (1) cause consumers significant injury, (2) not be reasonably avoidable by consumers, and (3) is not offset by countervailing benefits to consumers or competition.# Historically, the FTC has brought many cases against companies for failing to reasonably police the behaviors of others. For example, since 2002, the FTC has brought over 80 cases against companies for failure to institute reasonable security measures to protect consumers' personal information.[35] Even though the threat in those cases was from hackers and other malefactors, the FTC found that companies' failure to take cost-effective means to prevent those bad actors from accessing consumers' data constituted an unfair practice: it exposed consumers to the risk of significant injury, the poor security was not reasonably avoidable by consumers, and the failure to institute safeguards was not outweighed by other consideration. Similarly, the FTC could find that platforms' failure to protect consumers from bad actors by other users of the platform could also constitute an unfair business practice.

III. Algorithmic Accountability

As algorithms and artificial intelligence become more embedded into everyday decisionmaking, the potential for discrimination, misuse, and other harm is real and alarming. Algorithms can contribute to disparate impacts in areas like housing, credit, employment and also can contribute to exacerbated power dynamics between consumers and technology companies.

Engineers often use historical data when training algorithms to make decisions. For example, a company designing an algorithm attempting to predict where crime occurs most often in a city might use historical data about where crime has occurred most often in the past — however, this type of data could be skewed towards communities that tend to be over-policed;[36] algorithms like these can reinforce racial biases and exacerbate societal inequalities. Furthermore, many algorithms tend to be quite opaque — even to the engineers that design them.[37]

While discrimination is already prohibited in many sectors where algorithms are used, it can be difficult whether to tell whether algorithmic discrimination is ocurring at all due to the

[35] FTC, "Federal Trade Commission 2020 Privacy and Data Security Update" (2020) (online at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf)
[36] EFF, "Technology Can't Predict Crime, It Can Only Weaponize Proximity to Policing" (Sep. 3, 2020) https://www.eff.org/deeplinks/2020/09/technology-cant-predict-crime-it-can-only-weaponize-proximity-policing
[37] MIT Technology Review, "The Dark Secret at the Heart of AI" (Apr. 11, 2017) (online at: "https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/)

"black box" nature of many algorithms and the lack of transparency regulations. Consumers and citizens deserve explanations on how algorithms come to their decisions, particularly when used for sensitive applications; otherwise, progress made by antidiscrimination law will be heavily rolled back. People should also be able to contest inaccurate or false outcomes of an algorithm in a straightforward process.

Consumer Reports believes that we need increased regulation regarding algorithms which include increased transparency measures (on what kinds of data an algorithm uses and how the algorithm comes to a decision) to both the public and regulators, improved testing and auditing standards for algorithms used in areas with significant legal effects, and clearer restrictions on how and when certain algorithms can and should be used. We also need regulation that better outlines the rights of consumers and citizens when using the algorithms or when an algorithm makes a decision about an individual — including more individual agency of the use of algorithms, being given clear explanations about how a particular algorithmic decision works or how an algorithm arrived to its outcome, and being able to contest decisions.

H. R. 6580, The Algorithmic Accountability Act, is an important piece of legislation that can lay the foundation for these issues. While the bill doesn't necessarily require third-party auditing or other independent oversight over a company's testing process (something we think should happen with algorithms used in sensitive areas) or restrict when algorithms can be used, it does require companies to be more thoughtful about their design and testing processes. The various requirements that are discussed regarding a company's algorithmic impact assessment will force companies to consider things like stakeholder engagement, consumer rights in regards to opting-out or contesting algorithmic decision making, and potential negative impacts of the technology.

While stricter regulations are still needed to create better oversight and restrictions for algorithms used in various sectors, this bill is an important first step that can provide regulators and the public some transparency into how companies design and evaluate their algorithms. CR has put out a petition[38] urging Congress to pass the Algorithmic Accountability Act, and over 20,000 people have signed on so far. We urge Congress to pass this much needed piece of regulation which will lay the groundwork of making AI more safe and equitable for all.

IV. Surveillance Advertising

CR has long been a supporter of strong comprehensive privacy legislation. Last February, Consumer Reports released its Model State Privacy Act that strictly prohibits most secondary

[38] CR, "Cost of Love: Tinder charged higher price to older daters" (2022) (online at: https://action.consumerreports.org/20220209_finance)

data processing,[39] including for cross-context targeted ads.[40] In January of this year, we released a white paper along with the Electronic Privacy Information Center calling on the FTC to use its dormant rulemaking authority under Section 5 of the FTC Act to enact strong privacy rules that would likewise mandate strict data minimization and prohibit most secondary uses.[41] We see FTC rulemaking only as a fallback to Congressional action: Consumer Reports has previously testified before this subcommittee on the need for Congress to pass long-overdue legislation to clamp down on unwanted surveillance and unwanted ad targeting.[42]

We support the goals of the Banning Surveillance Advertising Act. Consumers overwhelmingly object to being tracked across different websites, apps, smart devices, and even in the physical world by hundreds of different companies just to show them relevant ads.[43] We appreciate that the bill is framed as a straight prohibition on surveillance advertising instead of conditioning it on opt-out or opt-in consent. In practice, opt-out rights under the California Consumer Privacy Act (CCPA) have proven to be burdensome and unworkable —it is not practical to expect consumers to navigate and manage hundreds or thousands of individual opt-outs for every site, app, or store they visit.[44] On the other hand, mandating opt-in for tracking creates burdens as well — in response to GDPR and the ePrivacy Directive, many sites forced users through tedious consent screens every time they visited a site, often using confusing language and "dark patterns"[45] to get a user to ostensibly provide "consent" to having their data shared with hundreds of companies. A simple prohibition on a universally despised practice is a better approach.

[39] By "secondary processing," we mean data collection, sharing, and use not strictly necessary to provide a service which a consumer has requested. If you buy a product online, your credit card number and home address may be collected and shared with a payment processor or a delivery service. However, these uses are "primary uses" are they're necessary to complete the transaction, and consumers generally understand what's going on. "Secondary processing," on the other hand, involves use and sharing for unrelated purposes, including sharing with data brokers and for targeted ads.

[40] CR Advocacy, "Model State Privacy Act" (Feb 2021) (online at: https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.)

[41] Consumer Reports and the Electronic Privacy Information Center, "How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking" (Jan. 26, 2022), (online t: https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf)

[42] Testimony of Justin Brookman, Director, Privacy and Technology Policy, Consumers Union, Before the United States House of Representatives Committee on Energy & Commerce Subcommittee on Digital Commerce and Consumer Protection, Hearing on "Understanding the Digital Advertising Ecosystem," June 4, 2018, https://docs.house.gov/meetings/IF/IF17/20180614/108413/HHRG-115-IF17-Wstate-BrookmanJ-20180614.pdf

[43] *E.g.*, Benson Strategy Group, Future of Tech Commission: Tech Attitudes Survey (July 20, 2021 - July 29, 2021), https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/pdfs/bsg_future_of_technology_topline_c1-1.pdf.

[44] CR Advocacy, "California Consumer Privacy Act: Are Consumers' Digital Rights Protected?" (Oct. 1, 2020), (online at: https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf)

[45] The term "dark patterns" refers generally to manipulative user interfaces designed to trick users into providing consent for potentially unwanted services or data processing. For more information see generally https://www.darkpatterns.org/.

However, focusing just on targeted ads is in our opinion too narrow an approach — there are tons of other ways that personal data can be collected and sold that intrudes on our personal spaces[46] and subjects us to adversarial uses.[47] We would prefer a more expansive bill that addresses surveillance beyond ad targeting. That said, stopping targeted ads alone is itself a worthy mission and would accomplish a lot of good for consumers beleaguered by constant tracking.[48]

Finally, we have some concerns about some of the loopholes and definitions in the bill that could ultimately undermine its effectiveness. For example, Section 2(a)(3) of the bill exempts ads based on information shared by advertisers themselves (or third parties on their behalf) to advertising facilitators. This provision would exclude much if not most surveillance advertising. Consider the canonical example of surveillance advertising: you browse a pair of shoes for sale, and then those shoes follow you all over the internet, showing up in ads on other sites, in other browsers, or even other devices. Here, because the data was shared by the shoe site to its partners in the ad tech ecosystem, it falls outside the protections of the act.

Similarly, the term "advertisement" is counterintuitively defined as:

> information provided by an advertiser to an advertising facilitator that the advertising facilitator, in exchange for monetary consideration or another thing of value, disseminates to an individual, connected device, or group of individuals or connected devices.

In practice, much of the information used for surveillance advertising is arguably not provided for consideration — instead, typically an advertiser gives *both* the data and money to an advertising facilitator in order to show an ad. It's the ad space that is sold, the data is just used to make the ad more targeted. In fact, advertisers adopted such an interpretation of the term "sale" under the CCPA that led to many ad tech firms simply declaring that their activities fell outside the scope of the law.[49] Unfortunately, experience has shown that privacy laws must be drafted extremely precisely, as companies have adopted bad faith interpretations of laws like the CCPA and GDPR, grasping onto dubious readings to preserve the status quo and avoid fundamentally

[46] American Civil Liberties Union, Face Recognition Technology, online at: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology.

[47] FTC, "*Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA"* (Jun. 12, 2012) (online at: https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed)

[48] Accountable Tech, "Re: Petition for Rulemaking to Prohibit Surveillance Advertising," (online at: https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf)

[49] Mediapost, "*Some Advertisers See Loophole in California Privacy Law*" (Oct. 22, 2019) (online at: https://www.mediapost.com/publications/article/342338/some-advertisers-see-loopholes-in-california-priva.html)

changing their behaviors. While regulators in both California[50] and the EU[51] have begun to take action to rein in the most absurd interpretations, many companies have been able to effectively skirt legislators' intentions by hiding in unintended loopholes.

V. Other Relevant FTC Powers and Authorities

Finally, for new laws to have any real impact on giant technology companies, regulators must be funded and empowered to take action. Today, the Federal Trade Commission has only 1100 employees to pursue both its consumer protection and competition missions.[52] This number has been roughly flat over the past twelve years, and actually represents a decrease from 1746 FTEs in 1979. Put another way, since that time, the economy has grown nearly three times while the FTC's capacity has decreased 37 percent. It is not reasonable to expect the FTC to be able to hold the biggest tech companies accountable on its current shoestring budget. Consumer Reports has consistently called for Congress to substantially increase the FTC's budget to give it the resources to bring on technologists and other staff to give the agency a fighting chance to achieve the goals for which Congress created it.[53] We are glad that [xxx bills provide for funding] they are a good start, but even more is needed.

And there must be consequences for companies that break the law. Today, when a company violates consumer protection law, the FTC largely has no ability to obtain any monetary relief at all from the company. After the Supreme Court's decision last year in *AMG Capital Management v. Federal Trade Commission*, the FTC does not even have the legal authority to get refunds for consumers who have been ripped off by fraudsters.[54] It is outrageous that scam artists are today legally entitled to keep their ill-gotten gains even after they are caught. Congress has the ability to enact a simple fix to the law to give the FTC the ability to obtain injunctive relief from wrongdoers, but so far it has failed to take action. Last year, Consumer Reports testified before this Subcommittee in support of the Consumer Protection and Recovery

[50] Digiday, "California Attorney General says popular, digital ad opt-outs from trade groups don't comply with CCPA" (Aug. 3, 2021) (online at: https://digiday.com/media/california-attorney-general-says-popular-digital-ad-opt-outs-from-trade-groups-dont-comply-with-ccpa/)

[51] IAPP, "Belgian DPA fines IAB Europe 250K euros over consent framework GDPR violations" (Feb. 5, 2022) (online at: https://iapp.org/news/a/belgian-dpa-fines-iab-europe-250k-euros-over-consent-framework-gdpr-violations/)

[52] FTC, "FTC Appropriation and Full-Time Equivalent (FTE) History" (online at: https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation)

[53] CR Advocacy, "Letter from Consumer Reports to Chairs Delauro and Quigley and Ranking Members Granger and Womack" (May 25, 2021) (online at: https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR-letter-on-FTC-appropriations-052521.pdf.)

[54] *AMG Capital Management LLC v. Federal Trade Commission*, __ U.S. __ (2021).

Act to restore the FTC's equitable authority; we strongly urge Congress to pass this simple fix to give the FTC what should be the least controversial tool it needs in order to protect consumers.[55]

Of course, even that authority will not be enough to deter wrongdoers — the FTC must be able to obtain statutory penalties as well. If the only consequence of getting caught is to refund what you stole, bad actors will take what they please, knowing that no regulator (even if fully funded) has the ability to catch everybody. Today, state attorneys general have the ability to exact civil penalties from companies that break the law; the FTC must be empowered to do the same. Otherwise, giant technology companies will feel comfortable pushing the boundaries of (or potentially just ignoring) laws intended to rein in their worst behaviors.[56]

[55] Testimony of Anna Laitin, Director, Financial Fairness and Legislative Strategy, Consumer Reports, Before the United States House of Representatives Committee on Energy & Commerce Subcommittee on Consumer Protection and Commerce, Hearing on "The Consumer Protection and Recovery Act: Returning Money to Defrauded Consumers," April 27, 2021,
(online at:
https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Laitin_CPC_2021.04.27.pdf)

[56] The FTC has been able to obtain civil penalties in a handful of cases against big companies, but only because those companies were caught violating settlement agreements they had previously reached with the FTC over earlier law violations. *E.g.*, Federal Trade Commission, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, July 24, 2019,
https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.. The FTC also has the ability to obtain civil penalties under certain sectoral privacy statutes such as the Children's Online Privacy Protection Act (COPPA). *E.g.*, Federal Trade Commission, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, September 4, 2019,
https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations. However, the considerable majority of the FTC's consumer protection cases are brought enforcing the general prohibition against "unfair or deceptive acts or practices"; in those cases, the FTC is not empowered to obtain penalties from wrongdoers.