Before the United States Senate Committee on the Judiciary,
Subcommittee on Subcommittee on Privacy, Technology and the Law,
Hearing on Platform Transparency: Understanding the Impact of Social Media

May 5, 2022

Statement of Daphne Keller
Stanford University Cyber Policy Center[1]

Chairman Coons, Ranking Member Sasse, and Members of the Subcommittee:

Thank you for the opportunity to testify. I am a legal academic, and primarily write about platform regulations, including international approaches, as they affect online content and speech. I also worked on transparency reporting at Google over ten years ago, and have more recently consulted or advised smaller platforms on their reporting, so I bring practical experience on today's topic.[2]

It is an honor to be here. I am particularly honored to testify alongside Nate Persily and Brandon Silverman. They have both built actual, working transparency tools – tools that can and should be expanded upon. The future should include more such tools. We should deploy more of the broad array of transparency mechanisms that I'm sure will be discussed in this hearing, including scraping tools, APIs, public repositories of data and content, and direct disclosures to individual users. The EU's new Digital Services Act (DSA) has prescribed many of these things by law. The U.S. can and should follow suit, enacting our own well-drafted laws to expand public understanding of major platforms' governance of online speech.

Transparency is essential to getting every other part of platform regulation right. I am grateful to the people who have put together proposals like the draft Platform Accountability and Transparency Act (PATA), the Digital Services Oversight and Safety Act (DSOSA), the NUDGE Act, and the Kids Online Safety Act for taking the first steps. But much as I'd love to spend my testimony cheering for transparency, I think my job here today is to point out difficulties that will need to be navigated if these bills are to reach their potential. I hope the drafters will take my comments as an act of support and an effort to make things better. At the end of the day, imperfect, first generation transparency laws may be better than no transparency laws. But they are also so important, it is worth the work to get them right.

There are a few things I see as gravely concerning in various proposals – elements that really don't belong in these laws, and could make them quite damaging. One is making transparency obligations a condition for immunity under laws like the Communications Decency Act provision commonly known as CDA 230. Connecting the two risks harming ordinary people, in ways that have very little connection with the goals of transparency laws. A second is drafting transparency laws in ways that effectively reduce people's legal protections from state

[1] Affiliation for identification purposes only; appearing in personal capacity.

[2] Recently I have consulted for Pinterest, including on transparency-related topics.

surveillance. A third is enacting transparency rules designed for giants like Facebook or Google, but imposed on very different and smaller companies.

Platform transparency in practice is complicated and messy.[3] If we ask companies for the wrong data, we won't learn useful things. It's hard to know in advance quite what the right questions are. Getting them right will be iterative, and what "right" means will almost certainly change with future technologies, business models, and human behaviors. Having an expert regulator to navigate those changes makes sense. But there are also major questions of policy that should be made by Congress. My goal here is to describe those as I see them, and to suggest some directions of travel.

Key Conclusions

High level takeaways from my testimony are as follows. Most of these are explored in more depth below.

- Transparency rules should be overseen by an expert agency with the flexibility to adapt to future changes, including technological ones. But that flexibility should be constrained by policy choices made by Congress. In some cases that may mean setting hard legislative limits, like rules limiting obligations to platforms over a certain size. In others, it may mean guiding the agency's choices by defining a list of factors it must consider, for example in weighing impact on competition against the public benefit of disclosures.

- Transparency laws should not become surveillance laws. Nothing in them should reduce Americans' legal protections under the Fourth Amendment or laws like the Stored Communications Act. Users' expectations of privacy should also shape any laws compelling platforms to report on those users' activity, including in cases where that activity was publicly visible.

- The privacy issues raised by researcher access to user data are complex and warrant both Congressional and agency attention. Laws requiring that platforms disclose user data to researchers present very serious tradeoffs between legitimate but competing goals. In many cases, there will be no way to support important research without compromising equally important protections for users. Some important underlying questions in this area would be better resolved through federal privacy legislation. Congress should engage with these difficult policy questions, consult with privacy and transparency experts, and provide guidance to implementing agencies.

- Broad public access to information is essential. Some of the most important research on platforms to date has been accomplished by researchers "scraping" publicly visible data from platforms, or using archives of material that are available to the general public. These approaches are not without privacy tradeoffs of their own. But there is inherent value in public data access, without federal agencies, companies, or universities acting as

[3] A list of concrete reasons why even basic accounting questions become complex is in Daphne Keller, *Content Transparency Logistics*, Stanford CIS Blog (March 19, 2020), https://docs.google.com/document/d/1tkZB3Hh73o9OzZzf6qMI8eN_eIX8fnRkUowzKxHURdk/edit.

gatekeepers. The complexity of privacy tradeoffs, and the imperfection of many potential resolutions, should not lead us to abandon efforts to expand and improve truly public access to information.

- Laws designed for a handful of megaplatforms should not automatically or easily extend to their smaller competitors. Treating smaller platforms like incumbents has consequences for competition, innovation, Internet users' rights, and public discourse. Any transparency laws should set careful thresholds in defining which platforms have enough users, revenue, or social impact to justify particular obligations. Hard policy calls about appropriate burdens on platforms should not be left entirely to agency discretion. At minimum, Congress should instruct agencies to consider factors like what risks platforms pose, what specific disclosures and burdens are appropriate as a result, and what research goals justify disclosure mandates. Agencies should perhaps also, to put it bluntly, experiment on the giants first. After familiarizing themselves with the mechanics of data collection and the complexity of privacy tradeoffs on platforms like YouTube and Twitter, as well as consulting with civil society and experts, regulators would be better positioned to tailor any obligations for other platforms.

- Transparency mandates should not be tied to immunities under CDA 230. The practical effects of this approach would likely disserve both transparency goals and the goals of CDA 230's critics.

- Transparency mandates raise several concerns about free expression and the First Amendment. One is that poorly devised rules may lead platforms to adopt blunter content moderation standards; stay out of the content hosting and moderation business entirely; or converge on similar rules that reduce the diversity of online speech. Another is that platforms themselves may raise significant First Amendment objections. Congress should be aware of and navigate these concerns.

- Platforms should not be liable for disclosures that are compelled by law. They should not be vulnerable to suit when they had no choice about providing data. If platforms' obligations are unclear, they should be able to seek agency confirmation about what actions are compulsory, and thus immunized. This principle applies both to affirmative disclosure obligations and to other important transparency laws, such as those governing scraping.

- The law should facilitate more open, ongoing communication between researchers, platforms, and the administering agency. Defining and collecting platform data sets can be complex, frustrating, and time-consuming. It requires clear and careful communication about technical details. Laws intended to enable data access and novel inquiry by researchers will serve all participants in the process better if they support collaboration and open discussion when possible. Any more adversarial process should be a fallback mechanism.

- U.S. law should be broadly aligned with the EU's new requirements under the Digital Services Act. I will describe those requirements below. Not all of them are cultural or constitutional matches for the U.S. But to the extent that our legal instruments can be reconciled, the result will be more useful information for the public and more consistent and streamlined obligations for platforms. It would also reduce the likelihood of future U.S./EU disputes about privacy and data protection in this area.

I. Privacy

One of the biggest policy issues for transparency laws involves user privacy. Some decisions, including about the data seen by researchers, involve complex tradeoffs. Other privacy issues should, I believe, be non-negotiable in transparency legislation. This includes preserving Internet users' existing protections from government surveillance.

A. Researchers' Access to Private Data

Some highly valuable research is difficult or impossible to carry out without researchers themselves seeing private information about Internet users. We cannot have both optimal research and optimal privacy: Lawmakers must make value judgments and tradeoffs between the two. Some of the issues involved would be better addressed by federal privacy legislation. In the meantime, transparency laws present thorny questions about what personal data researchers get to see. I explained these in detail in a recent piece, and will review them more briefly here.[4]

User privacy cannot be protected solely through after-the-fact liability for researcher misconduct, or data management requirements for things like secure storage or encryption. It also requires sensible rules about what data researchers see in the first place. While the details of such rules are best left to agencies, the policy direction should come from Congress. This could take the form of firm rules or more flexible factors to guide agency decisions.

- Private communications: To illustrate the issue, consider a project that involves content shared privately by users on a platform like Facebook. Disclosing the content of one-on-one messaging on the platform would be the modern equivalent of disclosing personal mail. Presumably Congress does not intend to depart so far from the spirit of the Fourth Amendment, or the letter of laws like the Stored Communications Act. (SCA) Should disclosure become more acceptable if a post was shared with twenty friends? With a hundred, or five thousand? Does the answer depend on the goal of the research and the sensitivity of the privately shared content?

- Sensitive content: Researchers do not need to know the identity of a user to uncover personal information when they review the content of privately shared posts. Such content may, for example, include breastfeeding images, or discussion of a named individual's personal struggles with cancer, bereavement, or difficult life choices. If researchers *can* see this content, user privacy is compromised. If they *can't* see it,

[4] Daphne Keller, *User Privacy Versus Platform Transparency*, Stanford CIS Blog (April 6, 2022), https://cyberlaw.stanford.edu/blog/2022/04/user-privacy-vs-platform-transparency-conflicts-are-real-and-we-need-talk-about-them-0.

extremely important research becomes impossible. In particular, if only platforms see the content they take down, they will continue to "check their own homework" in reporting on their content moderation practices. This could preclude third party researchers on foundational questions about errors, bias, or disparate impact of content moderation.[5]

- Large data sets: Similar problems arise with large data sets that are "anonymized" or show only aggregate data about users. As any privacy practitioner knows, it can be very easy to identify individuals' private information using such data sets. In the 1990s, for example, MIT researcher Latanya Sweeney used publicly available "anonymous" data sets to identify the health records of the governor of Massachusetts. More recently, researchers identified individuals based on their "anonymized" viewing data released by Netflix. These failings are better understood today. Technical tools like differential privacy or homomorphic encryption can help to avoid them. But those tools can also interfere with some kinds of research, including analysis of smaller or marginalized populations.

There are many other privacy questions of this sort. Should researchers have access to public posts that users have since deleted?[6] My tentative conclusion is that users should not lose so much control over their own posts. But that would make some bad actors online much harder to detect and study. Should an individual social media user's history of policy violations be made public?[7] Should transparency laws require platforms to track data about users or engagement, at the same time that many public interest groups want that tracking to stop?[8] If researchers who scrape social media content discover that a public figure used a pseudonym to discuss private topics in a public forum – like a Reddit support group for people struggling with infertility – should they be free to publish that information?[9] None of these questions are easy.

For some, the response to many of these questions is "Platforms can see this information anyway, and they use it for research. So it might as well be used for research in the public interest, too." Maybe that's the right way of looking at things. On the other hand, it doesn't track privacy laws' usual expectation (or perhaps legal fiction) that users consent to share their data with platforms based on particular expectations about how the data will be used, who will see it, how well it will be secured against breaches, and so forth. Unless user expectations and understanding shift significantly, that framework will be hard to reconcile with laws requiring platforms to hand users' data to third parties, for uses the person did not expect, under the

[5] Notably, the most important empirical research on content takedown policies comes from the rare cases where such content information *is* available to researchers, because it is public and remains available online. See discussion of Lumen Database in Daphne Keller and Paddy Leerssen, *Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation*, in Nathaniel Persily and Joshua A. Tucker, eds., *Social Media and Democracy*, Cambridge U.P., 2020, https://www.cambridge.org/core/books/social-media-and-democracy/facts-and-where-to-find-them-empirical-research-on-internet-platforms-and-content-moderation/78DE9202F2D00F2967EFC5CBDCE2CAF0.

[6] PATA Discussion Draft 12(b)(4) puts this decision in the FTC's hands.

[7] PATA Discussion Draft 12(b)(3)(F).

[8] DSOSA; PATA Discussion Draft definitions of reach and prevalence, and non-optional tracking at 12(b)(2).

[9] PATA Discussion Draft part 10(b)(3)(C) says FTC guidelines will tell researchers not to publish identifying information scraped from public sites without consent, except for public officials and public figures.

stewardship of less capable security teams. Mandates like this may also raise real tensions with the EU's General Data Protection Regulation (GDPR).[10]

Privacy challenges like these pose some questions that are technical, and appropriate for agency assessment. Recognizing when people may be reidentified using seemingly anonymous data sets, for example, is not a matter for Congress. Nor is the negotiation process that I think should precede any disclosures of private data to researchers. But other questions, involving values and public policy priorities, fit squarely in Congress's job description.

B. Government Access to Personal Data

Platform transparency laws should not create a back door for new government surveillance powers. It would be perverse if a bill intended to curb platform power instead became a means for state actors to harness that power, effectively using private platforms to collect information about citizens and bypass the Fourth Amendment.

To be clear, I do not think any U.S. bills are intended to have this effect. But careful drafting is necessary to ensure that they do not. This should include clear legislative statements that nothing about the new law will change or undermine users' protections from surveillance – in law or in practice. Additional fine-tuning of the legislation, in consultation with surveillance law experts, will also be needed to avoid unintended consequences.

Specifically:

- Any user information that platforms are compelled to share with researchers should not lose the legal protections it currently has under the Fourth Amendment, the SCA, or similar laws.

- By the same token, transparency laws designed to support public research should not create new obligations for platforms to disclose data to the government itself. If lawmakers believe such disclosures are needed, they should be achieved by other means, after open public debate.

- Lawmakers should think carefully about real-world dilemmas that will be encountered by researchers who obtain access to private data. If a researcher believes she sees evidence of a crime, for example, can or should she notify law enforcement? The possibility of information flowing to police in this manner should prompt careful Fourth Amendment

[10] This becomes relevant if, as seems likely, platforms cannot accurately exclude European users from disclosures – although, as discussed in the final section of this testimony, pending legal changes in the DSA may affect this analysis. Under any system, though, obtaining "consent" through unilateral notices to users does not strike me as a real cure. Such notices not only deprive users of the ability to opt out, but risk being either meaninglessly broad, or else so frequent they get ignored.

evaluation, and influence what data researchers see in the first place.[11] It should also influence any authority agencies have to approve research that targets individuals or small groups.

- Lawmakers should act with care in requiring platforms to neatly package and deliver information that is nominally public, but that would currently be more difficult to find or assemble. Friction and speed bumps in data collection matter for real-world privacy, and can matter in the law. Under the Fourth Amendment, for example, the fact that activity was carried out in public does not create unlimited license for law enforcement to use sophisticated tools like GPS location-tracking.[12] As a matter of public policy, civil liberties groups have consistently raised concerns about social media monitoring. Organizations like the ACLU have condemned the FBI's acquisition of software for monitoring public social media accounts, for example, as well as the Department of Homeland Security's previous practice of inspecting individuals' social media posts at the border.[13]

- Considerations about users' reasonable expectations of privacy for technically public material online should shape platforms' public transparency reporting obligations. To my mind, those expectations are at their weakest, and transparency is most appropriate, for communications like advertisements or posts from commercial publishers who actively seek public attention. Privacy concerns are much stronger for users whose posts are public simply because they did not understand the privacy settings on a platform like Facebook, or who have no reason to expect attention from anyone but a few people for a public Twitter account. The student who uses Discord to joke with friends about sports, or the LGBTQ+ kid using Reddit to cautiously explore new online communities, should not have to anticipate their every word being preserved under government mandate for future inspection. Such expectations have a documented chilling effect on online speech, and even on users' willingness to search for information on sensitive topics including health or birth control.[14] This chilling effect is not unique to highly private people. As someone with a Twitter following that is approaching PATA's 25,000 threshold for public reporting, I can confidently say that this reporting would change what I say online,

[11] This question intersects with evolving case law about the state actor status of private entities that receive information by government mandate. Researchers in this situation could potentially be deemed state actors, meaning that any information they obtain without a warrant may not be admissible in court.

[12] U.S. v. Jones, 56 U.S. 400 (2012).

[13] Aaron Schaffer, *The FBI is spending millions on social media tracking software*, The Washington Post (April 5, 2022), https://www.washingtonpost.com/politics/2022/04/05/fbi-is-spending-millions-social-media-tracking-software/; Center for Democracy and Technology, *Fighting Government Intrusions on Privacy and Free Speech at the Border* (2019), https://cdt.org/2019-annual-report/fighting-government-intrusions-on-privacy-and-free-speech-at-the-border-2019-annual-report/; Faiza Patel et al, *Social Media Monitoring*, Brennan Center (2020), https://www.brennancenter.org/our-work/research-reports/social-media-monitoring.

[14] Alex Marthews and Catherine E. Tucker, *Government Surveillance and Internet Search Behavior* (Feb. 17, 2017), https://ssrn.com/abstract=2412564; see also PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (Nov. 12, 2013), https://pen.org/chilling-effects (journalists report avoiding writing about terrorism); Jonathon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, Berkeley Technology Law Journal, Vol. 31, No. 1 (2016), https://ssrn.com/abstract=2769645.

> and prevent me from using the medium as a venue for casual back and forth with the old friends who made up my earliest contacts on the platform.

II. Costs and Competition

Platform transparency has benefits and costs. I am a big believer in the benefits, and have written about them for years.[15] The costs can be harder to spot, but are very real. That's not a reason to forego transparency, but it is a reason to assume a certain "budget" for transparency, and allocate it carefully for maximum public benefit.

Some of the costs are economic. Even tracking platforms' existing content moderation work can come with costs in rebuilding internal tools and expanding and retraining content moderation teams to track data. This can take time away from those teams' other very important priorities, including combating child abuse material or terrorist content online. Collecting expansive new categories of data, like the prevalence metric promoted by Facebook, can be particularly costly.[16] This metric requires quantifying an unknown: the amount of prohibited content that moderators *haven't* found yet. To do so, platforms may use techniques like extrapolating from sample sets evaluated by moderators. Carrying out such evaluation on an ongoing basis, across multiple user languages and diverse cultural contexts, can impose significant costs.

Those costs are particularly meaningful to platforms that cannot, like Facebook or Google, spend billions of dollars on content moderation. This includes platforms that would likely be covered under laws like PATA, based on their number of users.[17] The $3.7 billion that Facebook has reported spending annually on safety and security, for example, is almost as much as Snap's reported annual revenue,[18] and many times more than Reddit's.[19] It dwarfs the endowment of the non-profit that operates Wikipedia.[20] While imposing certain costs may be appropriate, imposing disproportionate ones may have real competitive impact: deterring investment in new platforms, rendering smaller companies less able to attract users, or making them more willing to accept an acquisition offer from an incumbent more capable of meeting these obligations.

[15] See, e.g., Keller and Leerssen, supra note 5.

[16] The pros and cons of prevalence as a metric are well discussed in Bradford et al, *Report Of The Facebook Data Transparency Advisory Group* (2019), https://law.yale.edu/sites/default/files/area/center/justice/document/dtag_report_5.22.2019.pdf.

[17] See Appendix I.

[18] Facebook publicly announced that it would spend more than $3.7bn (c.£2.65bn) on safety and security on the platform in 2019. E&Y, *Understanding how platforms with video-sharing capabilities protect users from harmful content online* (Aug. 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1008128/EYUK-000140696_EY_Report_-_Web_Accessible_Publication_2.pdf. In 2021, Snap recorded $4.1 billion in revenue. Snap Inc., Form 10-K (2021), retrieved from https://investor.snap.com/financials/sec-filings/default.aspx.

[19] Reddit reported $100 million in quarterly revenue in Q2 2021, implying $400 million annual revenue. James Vincent, *Reddit is now valued at more than $10 billion*, The Verge (Aug. 12 2021), https://www.theverge.com/2021/8/12/22621445/reddit-valuation-revenue-funding-round.

[20] Wikimedia Foundation, *Wikimedia Foundation reaches $100 million Endowment goal as Wikipedia celebrates 20 years of free knowledge* (Sept. 22, 2021), https://wikimediafoundation.org/news/2021/09/22/wikimedia-foundation-reaches-100-million-endowment-goal/.

Other potential costs involve speech and content online. A platform seeking to reduce reporting costs might, for example, adopt simpler, blunter speech rules under its Terms of Service, or simply enforce fewer rules. Efforts to standardize reporting across platforms can, deliberately or not, drive standardization of the underlying speech rules and reduce users' options to participate in diverse speech communities. This homogenizing pressure exists today from advertisers' transparency requests.[21] U.S. law should not provide similar impetus toward online speech monocultures.[22] In particular, lawmakers should be very careful not to prescribe standards based on Facebook that then reshape what their competitors do. It would be perverse if the recent stream of disclosures about Facebook's missteps led to laws inadvertently nudging other platforms closer to Facebook's business model.

Again, none of these concerns are reasons to forego transparency laws. Nor do they all pose questions Congress must answer before enacting transparency laws. Many are appropriate for agency resolution. If lawmakers delegate substantive transparency rules to an agency, they should do so with guidance about the costs to be considered and the benefits to be prioritized in allocating the transparency budget and shaping those rules. In addition to the big picture concerns outlined above, other considerations should include:

- What specific risks are involved in a platform's business? There may, for example, be more legitimate public interest in data about unsafe products on commerce-related sites; copyright infringement on music sites; pornographic or child-inappropriate content on image hosting sites; or disinformation on political discussion sites. The broader and non-risk-specific obligations that may make sense for de facto public forums like YouTube, Twitter, or Tiktok may not make sense for other kinds of Internet giants, like Amazon. They are also hard to justify for platforms where users typically discuss hotel reviews (like Tripadvisor), post software code (like GitHub), or share employment experiences (like Glassdoor). The same analysis may pertain for different parts of one platform. Broad transparency obligation may be harder to justify for Reddit forums about cooking or cats, for example.

- What specific transparency obligations are appropriate, given a platform's size and risk profile? This question should affect researcher data access, with questions of public importance taking priority over more frivolous research. It is also relevant for other kinds of transparency. One example is the ambitious vision in proposals like PATA for ongoing, real-time reporting of sample user content, accompanied by distribution metrics, audience records, and other internal data. Such an expensive undertaking is harder to

[21] World Federation of Advertisers, *GARM launches its first-ever measurement report for digital brand safety* (Apr. 20, 2021), https://wfanet.org/knowledge/item/2021/04/20/GARM-launches-its-first-ever-measurement-report-for-digital-brand-safety.

[22] Poorly designed transparency laws can also reduce technical innovation. This might happen, for example, if requirements to report on algorithm changes deterred platforms from experimenting with changes to reduce algorithms' disparate impact or the appearance of harmful content. It might also happen if growing platforms became dependent on vendors providing outsourced moderation and tracking services, and their product design or back-end engineering suffered technical "lock-in" as a result.

justify if it primarily provides better public information about the popularity of restaurant reviews, crafts projects, or Lizzo videos.

- Will a requirement cause platforms to collect user data they otherwise would not?[23] In addition to general privacy issues, this may raise particular concerns if a law causes platforms to collect data on race or other demographic information.

- Will public disclosures give bad or adversarial actors the information they need to game the system, avoiding platforms' mechanisms for fighting spam, coordinated inauthentic behavior, or harassment? This is, I believe, one of the most important concerns to be navigated in transparency proposals.

- Is information competitively sensitive? This may be the case with user traffic data or the details of ranking systems, for example. Some of this information may also currently be protected under trade secret law. Trade secret concerns should not necessarily be a barrier to some disclosures, particularly to researchers with strong confidentiality obligations. That said, vetting and legal obligations will be important in this context, given that academic researchers often move to jobs in the industries they have studied.

- What problems may be caused by disclosing content that platforms have deemed to violate the law or their policies? Researcher access to content is incredibly important, as I have discussed. In many cases even otherwise illegal content, such as material supporting designated foreign terrorist organizations, can and should be lawfully used for research purposes. Other content, such as non-consensual sexual images ("revenge porn," the legal status of which varies by state) seem less appropriate to disclose.

- What degree of precision is needed to support the public purposes of transparency? Given the complexity and risk of error in data collection – particularly for smaller companies – some tolerance for imprecision and revision in reporting may be appropriate. Not every mistake should be a violation of law or carry other drastic legal consequences, in particular the loss of protection under CDA 230.

- Will transparency obligations deter platforms from socially beneficial behavior? A law requiring disclosure of internal research, for example, could discourage platforms from analysis that may ultimately help to protect users or improve products. The same goes for algorithmic transparency mandates. A law requiring disclosure of internal debates over contentious issues could expose employee participants to online abuse or undermine deliberative processes and outcomes.

Again, the point is not that any of these considerations should prevail over transparency priorities. Nor is it that Congress must find a perfect answer to every question. Rather, it is that

[23] For example, in an effort to identify unique users under the PATA Discussion draft's definition of "reach"; demographics under 12(c) and (e); or engagement under the mandatory language at 12(b). Given many public interest advocates' goal of *stopping* platforms from optimizing for engagement, it is odd to require further investment in tracking it.

all of these concerns matter. They should be factors in assessing transparency proposals of all sorts – ranging from public reporting to vetted research to safe harbors for scraping.

III. Speech

Transparency laws are generally intended to improve public access to information. At the same time, they can create other risks to speech rights and the public information environment. I believe that better transparency is essential for wise platform regulation, and hope that well-drafted laws can navigate these risks.
First, as discussed above, is the risk that transparency laws will effectively drive standardization in content policies, and reduce users' options to choose among diverse speech communities. Importantly, this affects *users'* speech rights. If Congressional action effectively reshapes platform speech rules affecting lawful speech, it may be subject to constitutional challenges by users and platforms alike.

The second risk is that transparency laws will be vulnerable to First Amendment challenge by the regulated platforms. This is a major concern. In the case most squarely on point, from 2019, the Fourth Circuit struck down Maryland's disclosure requirements for online campaign ads. The Court cited multiple First Amendment concerns, including chilling effects, compelled speech issues, and insufficient fit between the law's goals and its broad transparency mandates. (Notably, many of the factors listed in the "Costs and Competition" section of this testimony are potentially relevant for these First Amendment questions about means/ends tailoring.) There is also a serious concern about the enforcement of seemingly neutral transparency mandates as a mechanism for state influence on online speech. This is similar to the concern historically raised by many Republicans about the Fairness Doctrine, and has more recently arisen in Twitter's objections to sweeping discovery requests made by Texas Attorney General Ken Paxton.

This is a key question, and not one that has been widely examined. In the only serious public analysis I know of, Santa Clara Law Professor Eric Goldman concludes that transparency mandates raise major First Amendment concerns.[24] If I were in the shoes of lawmakers or staff, I would be asking the amazing lawyers at the Congressional Research Service to examine these questions.

IV. CDA 230

Platform transparency obligations should not be tied to platforms' shield from liability for user speech under laws like CDA 230, as is done in some transparency proposals. One reason for this is practical. The data collection and disclosures contemplated by transparency laws are difficult to get right. Errors or disputed interpretations of the law are all but inevitable, even for the most well-intentioned companies. Smaller or less well-resourced companies, or those new to tracking data, are particularly likely to make mistakes – or to reduce and simplify their content

[24] Eric Goldman, *The Constitutionality of Mandating Editorial Transparency*, Hastings Law Journal (*forthcoming* in Vol. 73, 2022), https://ssrn.com/abstract=4005647.

moderation efforts in order to avoid liability risk. Transparency regimes should not have this effect, or expose platforms to unpredictable civil liability risk.

For plaintiffs' lawyers and platforms, a rule that caused platforms to lose immunities based on shortcomings in transparency reporting would create a sort of lottery. New opportunities for litigation would vary not based on considered public policy, but based on what transparency mistakes a platform happens to make. A reporting error involving consumer reviews could open the door to litigation by restaurants disputing a customer's online claims; an error involving algorithmic ranking might bring suits about which news sources platforms should prioritize. Platforms would have to litigate even frivolous claims past the motion to dismiss stage, creating incentives to settle improper, opportunistic claims.[25]

This litigation lottery is not anyone's idea of sensible CDA 230 reform. It would not create procedural avenues for legitimate defamation claims, as the PACT Act does. It would not create remedies for victims of particular and substantial harms, as laws like EARN IT and SESTA/FOSTA attempt to do. It would not limit major platforms' power over public discourse, as proposals from Senator Hawley have aimed to do. Whatever one thinks of any of these bills or their policy goals, they at least reflect considered approaches to addressing specific concerns. Puncturing immunity in response to transparency failings would create more of an arbitrary, shotgun blast approach to public policy.

Involving CDA 230 raises the stakes for transparency laws. It makes the cost of legislative mistakes much higher. Imperfect transparency reporting laws can still do a lot of good; they may not do too much harm; and most of those harms will fall on regulated companies that are comparatively able to advocate for their interests. Flawed approaches to platform immunity laws like CDA 230, by contrast, affect the general public. They can harm ordinary people who often lack the wherewithal to object through lobbying or litigation. One set of harms involves speech and access to information. Platforms concerned for their own liability have reason to simply ban broad swathes of controversial speech or honor inappropriate takedown demands.[26] The other harms involve people's economic and social participation. As recent experience has demonstrated, platform purges of speech can also be purges of people, leading to loss of such basic services as payment processing and messaging.[27] Transparency laws are not the place to tinker with overall platform immunities and risk such consequences.

[25] See discussion of litigation costs in Engine, *Startups,*
Content Moderation, & Section 230 (Dec. 9, 2021), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/61b26e51cdb21375a31d312f/1639083602320/Startups%2C+Content+Moderation%2C+and+Section+230+2021.pdf.

[26] James Ball and Paul Hamilos, *Ecuador's President Used Millions Of Dollars Of Public Funds To Censor Critical Online Videos*, Buzzfeed News (Sept. 24, 2015), https://www.buzzfeednews.com/article/jamesball/ecuadors-president-used-millions-of-dollars-of-public-funds (describing abuse of legal notices to silence reporting critical of Ecuador's president); Craigslist, *About: FOSTA* https://www.craigslist.org/about/FOSTA (describing Craigslist's termination of its online personal ads section in response to SESTA/FOSTA).

[27] Danielle Blunt and Ariel Wolf, *Erased–The Impact of FOSTA-SESTA and the Removal of Backpage*, Hacking // Hustling (2020), https://hackinghustling.org/erased-the-impact-of-fosta-sesta-2020/.

V. The EU's Approach in the Digital Services Act

The EU's new Digital Services Act (DSA) is a once in a generation overhaul of EU law governing intermediaries' handling of user content. A final version was announced in April 2022, but there is as yet no official draft, and a few details remain unclear. The law extensively regulates platform content moderation, as I described in a recent post. [28] Specific obligations vary considerably based on a platform's size and technical functionality.[29] Some of the DSA's most far-reaching obligations apply only to "Very Large Online Platforms" or VLOPs, with an EU monthly active user count that exceeds 10% of the EU population. This is currently defined as 45 million people. The equivalent percentage of the U.S. population would be about 33 million people. Attached to this testimony is a rundown of platforms that would likely be caught by various size thresholds.

The DSA includes numerous transparency provisions, many of which have analogs in U.S. proposals. While the final draft may vary in some detail, the basic requirements from earlier drafts are highly likely to persist. These include:

- Public transparency reporting. The DSA requires regular public reports showing aggregate data about content removals, user appeals, and similar issues; information about the number of moderators employed and their training and linguistic expertise; information about the use and claimed accuracy of filters and other automated content moderation tools; and information about monthly active user count. (Arts. 13, 23 and 33)

- Reporting to government about individual content moderation decisions. The DSA obliges platforms to notify users in detail about content moderation decisions that affect them. Copies of these notifications are also to be sent to the European Commission, which intends to include them in a database. (Art. 15)

- Recommender system transparency. Platforms must publish information about their ranking and recommendation systems, including explaining parameters, optimization criteria, objectives, and any options users may have to modify such systems. (Art. 24a, 29). The largest platforms must also "explain the design, logic and the functioning of the algorithms" to regulators upon request.[30] (Art. 31)

- Advertising transparency. Platforms must provide information directly in the user interface about the source and targeting of ads. (Art. 24) The largest platforms must also maintain ad archives, accessible via APIs, containing information including the advertisers' identity, the content or "creative" of ads, the dates ads ran, parameters for

[28] Daphne Keller, *What Does the DSA Say?*, Stanford Center for Internet and Society Blog (Apr. 25, 2022), https://cyberlaw.stanford.edu/blog/2022/04/what-does-dsa-say-0.

[29] For a preliminary breakdown of which entities are expected to bear which obligations is here, see Daphne Keller and Jan Jakub Przerwa, *DSA Duties by Entity and Size*, https://docs.google.com/spreadsheets/d/1rlFtpZmqiW4Vt1IQ54EaJUsk1XGFPzkDdCnLjF-xq3Y/edit#gid=0.

[30] Earlier DSA drafts anticipated an assortment of potential regulatory bodies. In the final draft, most of the regulatory power will sit with the European Commission, but since this is not finalized I refer to "regulators" broadly here.

user group targeting, total users who saw ads broken down by targeted group, and whether each ad was determined to violate law or platform policy. (Art. 30)

- Disclosures to users about content moderation. Platforms must detail their content moderation policies in Terms of Service, and provide information to users affected by moderation decisions as well as to users who report content for violating the law or platform policy. (Art. 12, 14)

- Disclosing internal data to regulators and researchers. Regulators have broad authority to require the largest platforms to disclose internal information regarding their compliance with the DSA overall. Platforms must also give researchers vetted by the regulatory authority with access to information relevant to the platform's "systemic risks." A key dispute between DSA negotiators was whether non-academic researchers would be eligible for such access. In all DSA drafts that I've seen, regulators are to vet *researchers* rather than *projects*, seemingly meaning that once an entity has been approved, the only real check on its data access arises if platforms formally object. The DSA contemplates future implementing rules to establish technical standards, rules for use of data, and protections for confidential information and security of the service. One of the most complex issues will be the reconciliation of these disclosures with the privacy and data protection provisions of the EU's General Data Protection Regulation (GDPR). A proposed Code of Conduct for this, from the European Digital Media Observatory, is expected soon.[31]

- Platform risk assessments, risk mitigation plans, audits, and regulatory oversight. The largest platforms regulated under the DSA must conduct annual risk assessments and create risk mitigation plans, as well as undergoing assessment by independent auditors. (Art. 27-28) The resulting reports must be submitted to regulators, and redacted versions must be released publicly. Regulators will also have extensive powers to demand additional information from platforms, perform on-site inspections, and otherwise carry out investigations. (Art. 50-58)

VI. Conclusion

No one likes to come to Congress with a complicated message – especially in the context of legislative changes that are overall positive. But the reality is that transparency reporting is very complicated, and the details matter. Congress is not the right place to sort through all of these details, or to anticipate every technological and economic shift that may reshape transparency needs in the future. It is, however, very much the right place to consider the major policy questions that underlie transparency mandates.

[31] European Digital Media Observatory, *Launch of the EDMO Working Group on Access to Platform Data* (Aug. 30, 2021), https://edmo.eu/2021/08/30/launch-of-the-edmo-working-group-on-access-to-platform-data/.

APPENDIX 1

Reported Monthly Active Usage Data for Content Hosting Platforms
Daphne Keller
April 29, 2022

This document aggregates reported U.S. usage data for certain platforms hosting user-generated content. Some figures are pulled directly from platform SEC filings and public statements, others draw on other public reporting. Extrapolations or assumptions are detailed in the footnotes. **User counts are notoriously unreliable, and different companies may define the metric differently.** Nonetheless, having at least a general idea of user count is important for proposals that would create different legal obligations based on this metric. This brief overview, prepared with the help of an RA, is intended to do that.

***

More than 25 million monthly active users in the US
Data is either included in, or easily extrapolated from, SEC filings and other platform public statements.

- Facebook: 262M monthly active users in the US & Canada.[32]
- YouTube: More than 100M US monthly active users.[33]
- Tiktok: More than 100M US monthly active users.[34]
- Snapchat: More than 97M monthly active users in North America.**[35]**
- Wikipedia: More than 97M US monthly active users.[36]
- Pinterest: 86M US monthly active users.[37]

[32] 2021 Meta 10K, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf. Meta also reports 3.59 billion global monthly active people, which includes users across Whatsapp, Facebook, Instagram, and Messenger. A more recent report suggests still higher figures. Meta, Earnings Presentation Q1 2022, https://s21.q4cdn.com/399680738/files/doc_financials/2022/q1/Q1-2022_Earnings-Presentation_Final.pdf.

[33] YouTube has more than two billion MAU globally. If at least 5% are from the US, then there are at least 100M US MAU. https://blog.youtube/press/.

[34] TikTok reported 100M US MAU in August 2020, and usage has grown significantly since then. Alex Sherman, "TikTok reveals detailed user numbers for the first time, CNBC. (Aug 24, 2020) https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html.

[35] Snap currently reports more than 97M daily active users in North America; North America includes Mexico, Canada, Central America. MAU is necessarily higher than DAU. Snap 2021 10K, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001564408/da8288aa-d492-4fd1-b6ce-62dce8206e9f.pdf.

[36] Wikipedia is accessed by 1.95 billion unique devices per month globally. If at least 5% of traffic is from the US, then there are at least 97M MAU from the US. Wikipedia Statistics, "Unique Devices," https://stats.wikimedia.org/#/all-wikipedia-projects/reading/unique-devices/normal%7Cline%7C2-year%7C(access-site)~mobile-site*desktop-site%7Cmonthly (last accessed Apr. 29, 2022).

[37] 2021 Pinterest 10K, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001506293/86557168-9b9a-48fc-be82-e9efb7354d2c.pdf.

- Twitter: More than 38M US monthly active users.[38]
- Linkedin: More than 30M US monthly active users.[39]

Likely more than 25 million monthly active users in the US
*Data is estimated based on SEC filings and other platform public statement*s.

- Wordpress: Likely more than 40M US monthly active visitors.[40]
- Reddit: Likely more than 40M US monthly active users.[41]
- Yelp: Likely more than 30M US monthly active visitors.[42]
- TripAdvisor: Likely more than 30M US monthly active users.[43]
- Discord: Likely more than 25M US monthly active users.[44]

[38] Twitter currently reports 38M US daily active users, and monthly active users is necessarily higher than daily active users. Twitter 2021 10K, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001418091/947c0c34-ca90-4099-b328-a6062adf110f.pdf.

[39] Currently, LinkedIn has 800M global members. https://about.linkedin.com/. In 2015 (before Microsoft acquired LinkedIn), LinkedIn reported 98M active monthly users globally. At the time, about 30% of total membership was in the US, so LinkedIn had around **3**0M MAU US in 2015. This number is likely much higher now, as total membership has doubled since 2015. LinkedIn 2015 10K, https://www.sec.gov/Archives/edgar/data/1271024/000127102416000035/a20151231-10xkdocument.htm.

[40] Wordpress has more than 409 million global visitors each month. If 10% of these users are in the US, then Wordperss has more than 40M monthly US visitors. https://wordpress.com/activity/.

[41] In 2018**,** Reddit had 430M MAU globally, a number that has likely significantly grown since then. If at least 10% of traffic were from the US, then Reddit would have 43M US MAU. Jacob Kastrenakes, “Reddit reveals daily active user count for the first time: 52 million” The Verge (Dec. 1 2020) https://www.theverge.com/2020/12/1/21754984/reddit-dau-daily-users-revealed.

[42] Yelp reports 33M monthly unique app visitors, 45M unique desktop web users, and 56M mobile web unique visitors globally. These numbers are not mutually exclusive. While these numbers are global, Yelp primarily focuses its business in the US and Canada, and so are likely reflective primarily of US users. Yelp 2021 10K, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001345016/6cfb0115-fe02-447b-a835-35393b9e7286.pdf.

[43] In 2019, TripAdvisor had 490M monthly users globally. If at least 6% were from the United States, then TripAdvisor would have 29.4M US MAU. TripAdvisor Investor Relations, “Online Reviews Remain a Trusted Source of Information When Booking Trips, Reveals New Research,” (Jul. 16 2019) https://ir.tripadvisor.com/news-releases/news-release-details/online-reviews-remain-trusted-source-information-when-booking. Note that monthly usage numbers have fluctuated significantly with the COVID pandemic. The latest 10K stated 2021 usage numbers were 73% of a comparable period in 2019. If current numbers are at 73% of 2019, TripAdvisor would have 357M MAU globally. If 8% are from the US, then it would still have more than 25M US MAU. TripAdvisor 2021 10K, https://ir.tripadvisor.com/static-files/3e32bcb6-bb03-47ea-bd68-e7a3e82c2d30.

[44] Discord reported 150 million monthly active users globally in July 2021. If 17% of these users are in the US, then Discord would have 25.5M monthly active users in the US. Scott Nover, “Once a go-to for gamers, Discord is vying to be a chat app for all,” The Verge (July 17, 2021) https://qz.com/2034087/chat-app-discord-is-shedding-its-gamer-roots/.

Less than 25 million monthly active users in the US
*Data is either included in, or easily extrapolated from, SEC filings and other platform public statement*s.

- Eventbrite: Less than 25M US monthly active users.[45]
- Bandcamp: Less than 25M US monthly active users.[46]
- Patreon: Less than 8M US monthly active patrons.[47]

Significant platforms for which adequate public data could not be found
This includes data on other platforms for which current US monthly active user data is not available or reasonably inferrable. Many platforms on this list may in fact have more than 25 million US MAUs.

Glassdoor: 67M unique monthly users globally.[48]
Vimeo: 260M registered users globally.[49]
Steam: 132M monthly active players globally.[50]
Nextdoor: 35.9M weekly active users globally.[51]
Github: 8.32M US monthly visitors in 2015.[52]
Telegram: 500M active users globally.[53]
Dropbox: 700M registered users and 16.79M paying users globally.[54]
Etsy: 90.1M buyers and 5.3 million sellers active globally.[55]
Tumblr: no recent public usage data available.
Twitch: no recent public usage data available.

[45] In 2021, Eventbrite facilitated more than 291M ticket sales globally. On average, this means 24.25M tickets were sold a month. Even if all sales were from unique users, this would mean that Eventbrite would have less than 25M monthly users globally. US usage would likely be significantly lower, as Eventbrite operates in more than 100 countries. Eventbrite 2021 10K, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001475115/210efa34-aec6-4da8-abd1-34c8669239f6.pdf

[46] In 2021, Bandcamp users bought 25.75M digital albums, tracks, vinyl records, CDs, cassettes, and t-shirts. If all of these were unique users, then Bandcamp would have 25.75M unique users a year globally; since Bandcamp is used in many countries outside of the US, US usage is very likely below 25M MAU. https://bandcamp.com/about.

[47] Pateron reports 8M monthly active patrons globally. https://www.patreon.com/about.

[48] Glassdoor, "40+ Stats For Companies to Keep In Mind for 2021," Glassdoor for Employers. https://www.glassdoor.com/employers/resources/hr-and-recruiting-stats/

[49] Vimeo 2021 10K, https://investors.vimeo.com/static-files/765f2b08-f4bf-4a8b-a625-1b9eaef1d6ec.

[50] Steam 2021 Year in Review, https://store.steampowered.com/news/group/4145017/view/3133946090937137590

[51] Nextdoor 2021 10K, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001846069/c9e1f04e-9b56-4300-ae46-45b7408c9d3b.pdf

[52] Usage has likely grown significantly since 2015, but no resources are publicly available to indicate by how much. Brian Doll, "A Closer Look at Europe," Github Community Blog (June 17, 2015). https://github.blog/2015-06-17-a-closer-look-at-europe/.

[53] Telegram Twitter Bio, https://twitter.com/telegram.

[54] Dropbox 2021 10K, https://dropbox.gcs-web.com/static-files/58450624-a3a9-4f41-a94a-8799456275d1.

[55] Etsy 2021 10K, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001370637/619701ee-f7dc-4baa-9463-4374cfcef85e.pdf.

APPENDIX 2

Online Platform Transparency Reporting: Research, Laws, Datasets and Policy Proposals
Daphne Keller
April 28, 2022

This document, prepared with the help of an RA, is a bibliography aggregating some of the many important sources of information on platform transparency reporting and researcher access to platform data. A primary source was the broader dataset provided by the Partnership for Countering Influence Operations, https://ceip.knack.com/pcio-baseline-datasets#transparency--data-sharing/?view_69_filters=%5B%7B%22field%22%3A%22field_443%22%2C%22operator%22%3A%22contains%22%2C%22value%22%3A%22%22%7D%5D.

Research on Platform Transparency Reporting

- Spandana Singh & Leila Doty, "The Transparency Report Tracking Tool: How Internet Platforms Are Reporting on the Enforcement of Their Content Rules," New America (2021) https://d1y8sb8igg2f8e.cloudfront.net/documents/The_Transparency_Report_Tracking_Tool_update_3-18-2021.pdf.
- Spandana Singh and Kevin Bankston, "The Transparency Reporting Toolkit: Content Takedown Reporting," New America (2018) https://www.newamerica.org/oti/reports/transparency-reporting-toolkit-content-takedown-reporting/.
- UC Berkeley School of Law Human Rights Center, "Digital Lockers: Archiving Social Media Evidence of Atrocity Crimes" (2021) https://humanrights.berkeley.edu/sites/default/files/digital_lockers_report5.pdf.
- Santa Clara Principles on Transparency, https://santaclaraprinciples.org/
- Tech Against Terrorism, "Transparency Reporting Guidelines" (2021) https://transparency.techagainstterrorism.org/.
- Trust and Safety Professional Association, "Transparency Reporting" https://www.tspa.org/curriculum/ts-fundamentals/transparency-report/.
- Facebook, "Charting a Way Forward: Online Content Regulation" (2020) https://about.fb.com/wp-content/uploads/2020/02/Charting-A-Way-Forward_Online-Content-Regulation-White-Paper-1.pdf.
- Secretary of State for Digital Affairs, "Creating a French Framework to make social media platforms more accountable: Acting in France with a European vision," (2019) https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf (pgs 20, 25, 26 discuss proposed regulation including a transparency requirement for ranking and content moderation).

- OECD, “Transparency reporting on terrorist and violent extremist content online: An update on the global top 50 content sharing services”, OECD Digital Economy Papers, (2021) https://doi.org/10.1787/8af4ab29-en.
- European Data Protection Supervisor, “A Preliminary Opinion on Data Protection and Scientific Research,” (2020) https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf .
- Integrity Institute, “Ranking and Design Transparency: Data, Datasets, and Reports to track Responsible Algorithmic and Platform Design,” (2021) https://static1.squarespace.com/static/614cbb3258c5c87026497577/t/617834ea6ee73c074427e415/1635267819444/Ranking+and+Design+Transparency+%28EXTERNAL%29.pdf.
- Amelia Pia Heldt, “Reading Between the Lines and the Numbers: An Analysis of the First NetzDG Reports,” (2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413677.
- Robert Gorwa and Timothy Garton Ash, “Democratic Transparency in the Platform Society, chapter in Social Media and Democracy: The State of the Field,” (2020) https://osf.io/preprints/socarxiv/ehcy2/.
- Daphne Keller, “Some Humility about Transparency,” The Center for Internet and Society (2021) http://cyberlaw.stanford.edu/blog/2021/03/some-humility-about-transparency
- Svea Windwehr and Jillian C. York, “Thank You For Your Transparency Report, Here's Everything That's Missing,” EFF (2020) https://www.eff.org/deeplinks/2020/10/thank-you-your-transparency-report-heres-everything-thats-missing.
- Mark MacCarthy, “Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers and Industry,” Trans Atlantic Working Group (2020) https://www.ivir.nl/publicaties/download/Transparency_MacCarthy_Feb_2020.pdf.
- Relevant laws:
    - Australian Code of Practice on Disinformation and Misinformation, Transparency Reports https://digi.org.au/disinformation-code/ (2021).
    - Canada Bill C-76, 2018 https://www.parl.ca/LegisInfo/en/bill/42-1/C-76. (social media platforms must create and publish archives of election and partisan ads).
    - European Parliament and Council of the European Union, Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, Article 7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.172.01.0079.01.ENG&toc=OJ%3AL%3A2021%3A172%3ATOC (requiring companies to report on removing terrorist content).

    - French National Assembly, "La Lutte Contre la Manipulation de l'Information" https://www.gouvernement.fr/action/contre-la-manipulation-de-l-information (requiring reporting on ads).
    - German Network Enforcement Amendment Act, https://perma.cc/7UCW-AA3A (requiring reporting on content enforcement)
    - India Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf (requiring reporting on enforcement actions).

Researcher Access to Data

- Caitlin Vogus, "Independent Researcher Access to Social Media Data: Comparing Legislative Proposals," Center for Democracy and Technology (Apr. 2022) https://cdt.org/insights/independent-researcher-access-to-social-media-data-comparing-legislative-proposals/.
- Caitlin Vogus and Emma Llansó, "Report – Making Transparency Meaningful: A Framework for Policymakers," Center for Democracy and Technology (Dec. 14, 2021) https://cdt.org/insights/report-making-transparency-meaningful-a-framework-for-policymakers/.
- Drs. Amy O'Hara and Jodi Nelson, "Evaluation of the Social Science One – Social Science Research Council – Facebook Partnership," Hewlett Packard (2019) https://hewlett.org/wp-content/uploads/2020/02/Facebook-Partnership-Final-Evaluation-Report.pdf.
- Zuckerman et. al, "New Approaches to Platform Data Research," NetGain Partnership (2021) https://www.netgainpartnership.org/resources/2021/2/25/new-approaches-to-platform-data-research.
- Gary King and Nathaniel Persily, "A New Model for Industry-Academic Partnerships" PS: Political Science and Politics, 53, 4, Pp. 703-709. Copy at https://tinyurl.com/ybqrtrsz (2019).
- Axel Bruns, "After the 'APIcalypse': social media platforms and their fight against critical scholarly research," Information, Communication & Society, 22:11, 1544-1566, DOI: 10.1080/1369118X.2019.1637447 (2019).
- Jef Ausloos, Paddy Leerssen, Pim ten Thije, "Operationalizing Research Access in Platform Governance: What to learn from other industries," (June 2020) https://www.ivir.nl/publicaties/download/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf.
- Creating a Platform for the Sharing of Sensitive Online Data: White Papers. https://securelysharingdata.com/whitepapers.html (Includes several papers. The proposed "Institute for the Secure Sharing of Online Data" (ISSOD) is a new initiative that aims to establish an institute to: (a) act as a data repository for large-scale social and digital

media data sets (b) provide a replication archive for large sensitive scale social and digital media datasets (c) establish a new "National Information Survey" that provide regular surveys to monitor trends in digital information consumption).

- Stanford HAI, "Building a National AI Research Resource: A Blueprint for the National Research Cloud" (2022) https://hai.stanford.edu/sites/default/files/2022-01/HAI_NRCR_v17.pdf .
- French Ambassador for Digital Affairs, "Facebook Ads Library Assessment" (2020) https://disinfo.quaidorsay.fr/en/facebook-ads-library-assessment.
- Mozilla, "Facebook and Google: This is What an Effective Ad Archive API Looks Like" (March 2019) https://blog.mozilla.org/en/mozilla/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/ .
- Daphne Keller and Paddy Leerssen, "Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation" (Dec. 2019) https://www.semanticscholar.org/paper/Facts-and-Where-to-Find-Them%3A-Empirical-Research-on-Keller-Leerssen/d7f89602d821a724a007375bd8ee4382b9930eaf?p2df.
- Association of Internet Researchers, "Internet Research: Ethical Guidelines 3.0," (2019) https://aoir.org/reports/ethics3.pdf.
- Microsoft and NYU Open Data Policy Lab. https://opendatapolicylab.org/ (Institute for enabling access to public and private data)
- Marco Gaboardi, James Honaker, Gary King, Jack Murtagh, "PSI: a Private data Sharing Interface," (2016) https://arxiv.org/abs/1609.04340.
- Brandie Nonnecke1 and Camille Carlton, "EU and US legislation seek to open up digital platform data," *Science* (Feb 2022). https://doi.org/10.1126/science.abl8537.
- Data currently available for researchers:
    - Facebook Ad Targeting Transparency Data Sets, https://research.facebook.com/blog/2021/02/introducing-new-election-related-ad-data-sets-for-researchers/.
    - Facebook and Instagram Research Initiative on US 2020 Presidential Election, https://about.fb.com/news/2020/08/research-impact-of-facebook-and-instagram-on-us-election/.
    - Solom Messing, Saurav Mahanti, Christina DeGregorio, Zagreb Mukerjee, Bogdan State, Bennett Hillenbrand, Chaya Nayak, Arjun Wilkins, Gary Kings, Nathaniel Persily, "Facebook Privacy-Protected Full URLs Data Set": https://solomonmg.github.io/pdf/Facebook_DP_URLs_Dataset.pdf (exposure data for widely-shared URLs).
    - Facebook Data for Good, https://dataforgood.facebook.com/dfg/about (data sharing with non-profits)
    - LinkedIn and World Bank Group, "Industry Jobs and Skills Trends," https://linkedindata.worldbank.org/.

- Microsoft and ODI Open Data Campaign, https://theodi.org/project/microsoft-and-the-odi-helping-bridge-the-data-divide/.
- NYU Political Ad Collector and Observer, https://engineering.nyu.edu/news/new-tool-analyze-political-advertising-facebook-reveals-massive-discrepancies-party-spending.
- Surya Mattu, Leon Yin, Angie Waller, and Jon Keegan, "How We Built a Facebook Inspector, *The Markup* (Jan. 2021) https://themarkup.org/citizen-browser/2021/01/05/how-we-built-a-facebook-inspector
- Mozilla, "Getting serious about political ad transparency with Ad Analysis for Facebook," (Feb. 2019) https://blog.mozilla.org/netpolicy/2018/10/18/getting-serious-about-political-ad-transparency-with-ad-analysis-for-facebook/.
- Rally Mozilla, https://rally.mozilla.org/ (allows you to "donate" your data to researchers).
- Twitter Archive at the Library of Congress, https://blogs.loc.gov/loc/2017/12/update-on-the-twitter-archive-at-the-library-of-congress-2/.
- Twitter Academic Research Product Track, https://developer.twitter.com/en/products/twitter-api/academic-research (provides enhanced data access for researchers).