Statement before the Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
On Platform Transparency: Understanding the Impact of Social Media

Privacy and Other Challenges for Mandated Internet Platform Disclosure

JIM HARPER
Nonresident Senior Fellow

May 4, 2022

The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed in this testimony are those of the author.

Chairman Coons, Ranking Member Sasse, and members of the subcommittee:

Thank you for the opportunity to testify before you today. I am Jim Harper, a nonresident senior fellow with the American Enterprise Institute and a senior research scholar at the University of Arizona's James E. Rogers College of Law. For a little over two decades, I have been a policy analyst specializing in the intersection between technology and society. My major area of focus has been privacy, with forays and necessary study in a number of other areas, including transparency, telecommunications, counterterrorism, cryptocurrency, and more.

Executive Summary

There is a great deal of appeal to having greater transparency in all our institutions, including internet platforms. I have some experience with trying to create transparency one place where it lacks: in the US federal government. My experience is that it is hard to create usable transparency.

The mode adopted in legislation such as the proposed Platform Accountability and Transparency Act (PATA)[1] is to mandate disclosure on the part of platforms for the benefit of government-approved researchers and research projects. Under the bill, the National Science Foundation (NSF) and a new office in the Federal Trade Commission (FTC) would administer these mandates, including through the creation of privacy and cybersecurity standards for disclosure and disclosed materials.

Privacy is a complex value, though. In its control sense, it is lost when people's judgments about sharing and hiding information about themselves are defeated. I believe that an emergent property rights regime for data represents a substantial protection for privacy that people are already using in their interactions with internet platforms. By mandating disclosure from these platforms contrary to the agreements between platforms and users, the PATA legislation cuts against the grain of this kind of privacy protection. The legal immunities in the PATA legislation further erode confidence that privacy will be protected in a mandated disclosure regime.

An unconstrained disclosure mandate may be unconstitutional, and it seems unwise. The Supreme Court appears likely to revive the nondelegation doctrine soon, and an unrestricted grant of authority to mandate disclosure for the all-purpose, nebulous goal of transparency may not survive it. Constraints on the authority to mandate disclosure would be for the good. The beneficial possibilities of such mandates while our politics are generally healthy should not obscure the malign potential of mandated disclosure when our politics are less healthy.

In any event, platforms' moderation strategies and tactics should not be made transparent. Doing so

would make moderation more difficult and likely degrade the experience for platforms' users. The same logic applies to security, both the security of platforms themselves and the security that platforms seek for their users. Mandatory disclosure of security information could threaten platforms and their users.

Mandating general transparency has little precedent in our law that I am aware of. Businesses in all but a few exceptional lines have constitutional rights against being inspected or searched without warning or reason. When the business is communications, the First Amendment makes the idea of a general warrant to mandate disclosure all the more alien.

The better approach to platform transparency is to pressure platforms in ways other than through government coercion. They should participate with researchers in discovering their own consequences for society. They should seek to correct and improve where they can. To reduce the constraints that could prevent platforms from participating in research, amendments to the Computer Fraud and Abuse Act (CFAA) may be warranted to protect researchers from distended legal threats against their efforts to examine the functioning of platforms. The United States should avoid highly restrictive European-style privacy regulation in favor of our harm-based approach.

A substantial section below endorses the premise stated first above that transparency is good, but I begin with privacy and the privacy costs of a mandated disclosure.

Privacy and Related Values

An important cost of mandated disclosure would be to the privacy of platforms' users. Privacy is a complex value or set of values, so I will delve into it at some length, articulating how privacy is threatened and arguably violated even when mandated disclosure is joined with protections like those seen in the PATA legislation.

One hears appeals to privacy in many different policy and social contexts. My assessment is that people use the word "privacy" for eight distinct values.[2] Those values, in brief, are:

- **Control of Others' Access to Personal Information.** For countless reasons, including having a sense of control, people prefer to keep some information about themselves from others.
- **Fairness.** Each individual should get their due, whether their due is opportunity and promotion or punishment and loss.
- **Personal Security.** Denying others information about oneself can protect against physical threats and violence.

- **Financial Security.** Withholding information can be a preventive of financial frauds such as identity theft, in which someone impersonates someone else, creating accounts and debts in the victim's name.
- **Peace and Quiet.** People want to enjoy a sense of retreat from the world.
- **Autonomy.** The availability of information about people is an essential tool of legal and social pressure that may restrict people's freedom to act.
- **Integrity Against Commodification (or Anti-Commercialism).** Many people resist what seems to be the commercialization of everything and their own commercial objectification, preferring to be treated as whole individuals.
- **Reputation.** People worry that negative information about them will create negative impressions and adverse social and economic treatment.

In survey research I recently published,[3] I found that financial security (i.e., prevention of identity fraud) is foremost in people's minds when asked an open-ended question about privacy concerns. When prompted to address the eight values listed above, financial security remains a top priority, joined by personal security, reputation, and autonomy. Lower-tier values, in descending order, are control, fairness, peace and quiet, and anti-commercialism. This is disappointing in a sense. Many of the lower-tier values are upper-tier for people like me. For me, the picture this research paints is of Americans as busy, practical people, who want what they want. They don't want to be scammed or injured, but they don't care that much about getting the kid-glove treatment in the information economy that we elites would like them to have.

I will focus here on what I believe to be the strongest sense of the word "privacy": control of information about oneself. A legalistic definition of privacy in the control sense that I worked up some years ago has held up fairly well. Privacy is "the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values."[4] We all hide and share information about ourselves to portray ourselves as we wish to be perceived by others. Most people do so inarticulately, following social customs and the occasional lessons of trial and error.

Importantly, privacy is subjective. Each person chooses what to share and what not to share (again, inarticulately) based on their own interests, values, customs, and so on. Overriding their choices deprives them of control and thus privacy.

An illustration: We all retreat into our homes to gain privacy (in the control sense, as well as the "peace and quiet" sense). If a government agency—say, local police or fire—installed camera systems in each home to improve emergency detection and response, this alone would violate privacy, even before any improper use of the system. Policies designed to prevent error and abuse could reduce various risks, but it would not alter the fundamental divestment of control from the residents of the home to another decision maker. Such monitoring could only be installed consistent with privacy if the people using the four walls of the home to protect their privacy assented to this modification of their information environment.

I use an example from the physical environment because it is familiar. We all find it easier to protect privacy in physical environments because they have been around for a long time. We understand how light and sound work, and customs are stable. It is relatively hard to protect privacy online because the environment is new and still rapidly changing. The technology is complicated, and there is not a stable set of customs people can draw on to protect their privacy. But there are protections for online privacy that I think are important to recognize.

Privacy Protection Through Contract and Property

I have argued for some time in various writings[5] and in legal briefs to the Supreme Court[6] that there is more privacy protection online and in the communications world than many people recognize. In my view, privacy policies and terms of services statements are contracts that not only commit service providers to baseline privacy-protective behaviors; they also divide up ownership of data.

Data—this stuff that people and companies trade, own, subdivide, and profit from—is an emergent form of property. Recognizing data as property will strengthen people's privacy protections because their loss will be more clear and they will have more remedies when, too often, some form of breach, unconsented sharing, loss, or harm occurs. If I am right that data is an emergent form of property, taking it by fiat implicates the same legal challenges as taking tangible items or land.

In the mid-to-late 1990s and early 2000s, as the internet was only beginning to become the commercial and social juggernaut that it is, foresighted legal scholars focused on the impending problem of privacy protection.[7] They recognized the internet as a giant, pervasive information-collection machine, and many believed it threatened doom for people's control of information about themselves.

Legal scholars with a taste for economics suggested protecting privacy by "propertizing" personal information. Giving consumers property rights in information about themselves would strengthen their

hands in the battle to protect their privacy. Others lamented that idea for a variety of reasons, including that it would "normalize" trade in data and undermine privacy (elite defined) yet further. Today scholarly consensus may be that property rights in personal information remains an interesting idea with plenty of complexity and as many drawbacks as benefits for privacy protection.

I think about these things a little differently. I believe that personal information has already acquired the characteristics of property and should be recognized as such. Companies and consumers routinely hoard or withhold personal information, process it, trade it, and enjoy other rights to personal information that are in the "bundle of sticks" that make up property rights.[8]

An empirical study has shown that courts increasingly recognize privacy notices as contracts.[9] And the Supreme Court has treated information as property. In a 1987 case called *Carpenter v. United States*,[10] the Court found that a scheme to trade on information awaiting publication in the *Wall Street Journal*'s "Heard on the Street" column deprived the *Journal* of "money or property" for purposes of federal mail and wire fraud statutes. "The Journal had a property right in keeping confidential and making exclusive use, prior to publication, of the schedule and contents of the 'Heard' column," Justice Byron White wrote for a unanimous Court.[11] That was so because, even though there was no prepublication release of the information, the fraud deprived the *Journal* of its exclusive control and disposition of the information—the rights to exclude others from, and to use, the information. This protection for a corporate entity's information should apply equally to ordinary people's information, in my opinion.

In a more recent and—to privacy people—more familiar *Carpenter* case, Justice Neil Gorsuch argued for treatment of personal information held by telecommunications companies in property terms.

> Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a bailment. A bailment is the "delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose." A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the "implication[s] from their conduct" if they don't. A bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable for conversion.[12]

In another Fourth Amendment case called *Riley v. California*, the Court wrote of a phone's contents as "a person's private effects."[13] The Court spoke of digital materials as owned items consistent with the

possessive pronoun “their” in the Fourth Amendment. We do not have to create a property regime for personal information. We just have to look around.[14]

Consider how privacy policies and terms of service statements allocate rights in digital data between service providers and customers. The heart of the typical privacy policy says something like: “Verizon does not sell, license, or share information that individually identifies our customers, people using our networks, or website visitors.” There is typically a short list of exceptions allowing sharing for such things as protecting the service provider, counteracting fraud, responding to valid legal process, and so on. These are the metes and bounds, covenants and easements of digital property, if you will.

When technology users leave data in the possession of service providers, all is not lost for them. According to their contracts, the general right to exclude remains theirs, an essential privacy protection.

Like spectrum, information is highly divisible, and it has different characteristics from movable and real property. (In their time, movables had to earn full-fledged status as property.[15]) As noted above, property rights include the right to possession, the right to use, to profit, to sell, and especially to exclude others. People and businesses exercise all these rights over data all the time.

There are several advantages to recognizing data as property allocated in part to consumers when they interact with service providers. Those advantages range from principled to practical, concrete to speculative. A principled argument is that it is consistent with Anglo-American common-law rule development to do so. Whatever scholars think or say, real people and companies talk about personal information as property. Across the internet, terms of service and privacy policies use possessive pronouns—“your information”—to describe this thing. What the contracts say is the best evidence available of what people think. And it is in the spirit of the common law to recognize this broad and deep cultural belief, incorporating it formally, if carefully and selectively, into the law.

The practical arguments are naturally more accessible. Treating personal information as property expands the range of remedies and protections that are available to consumers in a variety of situations, such as bankruptcy and contract breach. Most importantly to me, recognition of property rights in data would cause the standard privacy policy to establish that personal information in the hands of online service providers is the user-consumer’s. This data is part of people’s modern “papers and effects” for purposes of Fourth Amendment administration. Data about us in the hands of third parties is not so much soup to be ladled out by governments as soup from a tureen.[16]

Mandated Disclosure Undercuts Privacy

The move to mandate disclosure of personal information in the PATA legislation cuts deeply against the grain of this trend. It would signal that the US Congress sees personal information held by platforms, under contracts restricting others' access, as just so much soup awaiting the ladle.

This is true even when, as in PATA, the information will be subject to a regime of privacy and security protections. Like the placement of cameras in a home, taking data from where a consumer has deposited it and placing it in a different system divests the consumer of control. We do not have to love platforms' records on privacy to recognize that consumers have made choices and to respect their choices.

I recommend against mandating disclosure of information held by platforms despite the gains on offer for platform transparency. Doing so would undercut privacy and emerging property rights that are very important consumer protections.

Generous Immunities Undercut Privacy Protection, Too

Reading the PATA bill for the first time around Easter, I was impressed by how it distributes legal immunities like Easter eggs. Insulating particular groups from general law can be justified by a compelling interest, but it comes at a cost, and doing so is rightly controversial.[17] I believe immunities should be used more sparingly, if at all, in the legislation.

Section 6(d) of the PATA bill immunizes platforms that comply with the privacy and cybersecurity regulations from suits grounded in their disclosure of the mandated information. Researchers get their immunity in section 7(d), also contingent on compliance with the privacy and cybersecurity regulations. These immunities create a simple but concerning dynamic: If the FTC regulations meant to protect disclosed information do not protect privacy and security in some respect, and if harm comes to consumers whose data has been shared under PATA, those consumers will flatly be denied recourse. The distribution of immunities in the bill says that it is more important to subject people to interesting research than it is to accord them justice when they are wronged.

In section 11, civil and criminal immunity extends to people gathering "covered information" (a defined term) if they are engaged in news-gathering or research projects "to inform the general public about matters of public concern."[18] This would draw courts into assorting liability based on what constitutes "public concern," which is a social judgment courts are not well positioned to make. Indeed, it is essentially content-based assignment of immunity, which should fall afoul of the First Amendment.

Researchers without an approved focus could be sued. Researchers who meet with government approval could not.

My guess and sense as a nonexpert in this particular area is that the section 11's immunity aims to shield good-faith researchers from the CFAA. That law appears to suffer from unclear definitions, to wrongly treat civil wrongs as criminal, and to impose heavy-handed criminal penalties. If that is the purpose of this immunity, I recommend fixing the CFAA directly. Doing so would be much better than creating a complex carve-out from a complex legislative rule.

The PATA bill doesn't stop at allocating immunities. It also withdraws a sort of immunity from misbehaving platforms. Section 10 of the bill denies the protections of the Communications Decency Act's section 230 (CDA 230) from platforms that do not share information as required by the FTC under PATA. (It is narrow: The failure to comply with PATA would have to be a "significant contributor" to the claim against which CDA 230 no longer immunizes.) All this invites a brief discussion of how the CDA 230 "situation" might have been handled better.

Having worked around Congress for 25 years (and meaning no offense), I think it is better to arrive at just rules through long, society-wide deliberation than through legislative debate.[19] CDA 230 illustrates why.

In the mid-1990s courts were considering whether interactive online services would be considered publishers of the information people uploaded and posted to them. If they were publishers, website operators might be liable for defamation and other causes of action because of the material users contributed to them. Had this rule taken hold, operators of online services would probably have allowed only tightly controlled and monitored interactions among users. The rollicking, interactive internet we know today would have been sharply curtailed.

In response to this concern, Congress passed legislation saying that interactive computer services are not publishers or speakers of any information others provide using their services. Thus CDA 230 became one of the most important protections for online speech in the United States.

Though it is technically a substantive definition, CDA 230 acts as an "immunity" Congress gave to online service providers. The perception of CDA 230 as a special-interest favor means that other interests are on relatively strong footing when they come to Congress seeking to overturn it. Today, CDA 230 is under attack from groups who would like to see it weakened or reversed, perhaps including one or more members of this panel.

I believe the rule against liability for online service providers is the correct one. It would be stronger if courts had arrived at a rule of "no liability" based in considerations of natural justice.

When the rules that organize our society are temporal products of legislation, they may always be "in play" for a legislative reversal. Because of CDA 230, online service providers must always remain vigilant in Washington, DC, for attempts to undercut their special "immunity." The rules that govern online liability were established quickly, which is good, but they are obviously not settled, and there is one more reason for private businesses to maintain a stable of lobbyists and lawyers in Washington.

There is no guarantee, of course, that the common-law rule would be the same right now as what CDA 230 produced. The common-law process might still be searching for the right rule. I suspect that the platforms would not have quite the "blanket" protection that CDA 230 offers. There would be finer lines determining whether and when they are liable for the content they host. But my main point is that immunities have the effect of trampling through issues that we have a good system for analyzing: our common-law courts. They are an important part of the Anglo-American legal tradition, which is unwisely dismissed.

My strength and focus, as noted earlier, is privacy. I'm evidently willing to share opinions about other matters based on familiarity or even mere awareness. I have reservations about advancing transparency through mandated disclosure. I don't think the trade-off between privacy and transparency on offer in PATA is a good one. But I am cognizant of the value of transparency. I have worked to create transparency in one of our nation's largest institutions. And I know some of the difficulties involved in producing it.

We're All in Favor of Transparency

It is easy to favor transparency in our institutions. But it is a somewhat slippery concept. It may be widely popular simply because anyone can see it is a means to their own ends. But there can be too much of a good thing. The boundless transparency sought by the PATA bill may be ill-advised and prospectively unconstitutional. Below I recommend withdrawing data pertaining to platforms' moderation and security protection from mandatory disclosure.

Three years before ascending to the Supreme Court, Louis Brandeis wrote, "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."[20] He was arguing in *Harper's Weekly* (December 20, 1913) for measures that would weaken the power of investment bankers. His focus on

publicity (in a sense equivalent to "transparency" today) may have been a counterpoint to his earlier *Harvard Law Review* article[21] written with Samuel Warren entitled "The Right to Privacy."[22]

One can see broad parallels between the Progressive Era's concern with financial and industrial trusts and modern concerns with "Big Tech." Your evident concern with social media's pathologies line up, semantically at least, with Brandeis's "social and industrial diseases."

But the sunlight metaphor has an older pedigree. Professor Alasdair Roberts of the University of Massachusetts Amherst believes that Brandeis picked it up from James Bryce's 1888 book *The American Commonwealth*.[23] "Public opinion is a sort of atmosphere, fresh, keen, and full of sunlight, like that of the American cities," Bryce wrote, "and this sunlight kills many of those noxious germs which are hatched where politicians congregate."[24]

Brandeis saw transparency as a corrective for corporate and financial wrongdoing. Bryce saw transparency as a corrective for political wrongdoing.

Their differing emphases illustrate both a strength and a weakness of transparency as a policy objective. The strength is that transparency is easy to support. It as an empty vessel into which anyone can pour their priorities, just as Brandeis and Bryce did. Conservatives and liberals may agree on platform transparency because they each foresee the other's ox being gored in new light.

The weakness of transparency is the other side of the same coin. Favoring transparency is a commitment to no particular end. The devil in the details is the end (or ends) to which transparency may be put.

For a time, my work focused on transparency to a degree that I might have been characterized as a transparency activist.[25] President Barack Obama's election in 2008 began a period of focus on government transparency. His campaign promises related to transparency of governmental operations and decision-making were exciting and encouraging. I sought to contribute to the nonpartisan and pan-ideological effort in the nonprofit sector to advance US government transparency.

Having started down the path to digital transparency some years before with a (now-defunct) website called WashingtonWatch.com, a decade ago I created and ran a project at the Cato Institute called "Deepbills."[26] The project sought to enrich the publication of congressional legislation in Extensible Markup Language, or XML. XML is an encoding technique that can make the meaning of content such as bill texts automatically legible via computer.

Because of that project, for a brief period in 2014 one could look online to find the bills in Congress that

authorized appropriations or appropriated funds. You could see what members of Congress proposed to spend, and you could sort spending bills by dollar value, by date of last activity, and by the author's state.[27] Encoding bills in this way could only be partially automated, and the process of hand coding thousands of your lengthy bills was prohibitive, so the project ended years ago without leaving much of a mark. (The effort that did make a mark—and continues to do so—is Josh Tauberer's GovTrack.us.[28])

An uncomfortable parallel preceded the failure of my transparency project: The first broken promise of the Obama presidency was about transparency. In campaign speeches and on his campaign website, President Obama had pledged to put the bills Congress passed online for five days before signing them. This would give Americans a chance to find out what was in them before they became law, an arguable check against unwanted material being "snuck" into large bills. But President Obama signed his first law, the Lilly Ledbetter Fair Pay Act, just one day after Congress presented it to him.[29] The White House website asked the public for online comments two days after the bill became law.[30] As a set of institutional behaviors and public expectations, transparency is hard to manufacture.[31]

The audacious "whole of government" to "whole of the public" transparency we tried to create was "pro-democracy" and agnostic as to outcome. My view was that it might decrease demand for government. Others believed, I'm sure, that it would validate and perhaps grow existing programs and spending. It is no wonder that I focused on government spending data while others focus on campaign spending data. We were each seeing in transparency different ends that depended on our ideological starting points.

So transparency is essentially question-begging. As the subject matter of institutional transparency becomes more focused, harder questions arise. I will explore the decisions you *haven't* made in PATA's press for platform transparency through a brief diversion into constitutional nondelegation principles.

Uncircumscribed Authority to Promote Research Is Unwise

The strength of transparency as an all-purpose good thing may be a constitutional weakness. PATA creates an executive branch office and legal authorities to promote platform transparency by mandating disclosure of data to researchers. Without clear direction about precisely what should be subjected to research, PATA may fall afoul of the requirement that Congress must set policy priorities and not leave it to executive branch agencies or others.

Sections 4(d)(1) and (2) of the bill require the NSF to produce a list of "its criteria" for qualified research projects and qualified data and information. I perceive no subject-matter limit on the power the

legislation would give the NSF to authorize research projects that use platforms' data, which section 6(a) requires them to turn over.

There are many legitimate concerns with social media platforms. The press statement issued when the PATA legislation was announced makes reference, variously, to "tradeoffs," sex trafficking, information about COVID-19's origins, harm to "our families, our communities, and our democracy," and threats to "our democracy and the information ecosystem."[32] The legislation does not restrict NSF-sponsored research to these topics.

As time and presidential administrations unfold, areas for research could include literally anything under the sun: immigrants' use of their native languages on social media, small businesses' customer cultivation practices, churchgoers' illicit online relationships, LGBTQ+ political organizing, drug culture and consumption in ethnic and racial communities, gun afficionados' social ties, how heterodox ideas propagate online, and more. Not all this research may be tuned to fostering the well-being of the communities under examination. The point here is that an open-ended research agenda is open-ended. If some of the research topics I have listed alarm or offend you, note that PATA excludes none of them.

Section 12, giving the FTC authority to require reports and disclosures from platforms, is similarly open-ended. Subject to privacy limitations, whatever "will assist the public, journalists, researchers, the Commission, or other government agencies" to "assess the impact of platforms" on "consumers, institutions, and society" is fair game for required disclosure. This pro-transparency policy is boundless.

"Nondelegation" is the idea that the Constitution, having granted Congress the authority to legislate and set federal policy, bars Congress from sub-granting that authority to another body, whether within the government or without. The doctrine has largely been moribund since the New Deal. But three years ago, the Supreme Court decided a case called *Gundy v. United States*.[33] The case itself did not revive the nondelegation doctrine but signaled that the Court will do so soon.

Dealing with the interpretation of a sex-offender registration statute that arguably gave the US attorney general too much policymaking authority, the case was a 4–4 decision on an eight-member Court. Justice Samuel Alito, providing the fourth vote to uphold the statute against a nondelegation challenge, said he was unwilling to revive the nondelegation doctrine without a full complement of justices, but he would join a full-Court majority willing to revive it. Since then, the membership of the Court has returned to nine, and the makeup of the Court has shifted so that there is likely a nondelegation majority for Alito to join.

The contours the doctrine will have when it is renewed are not entirely certain. Justice Elena Kagan, writing for the plurality (i.e., upholding the law), wrote:

> [T]his Court has held that a delegation is constitutional so long as Congress has set out an "intelligible principle" to guide the delegee's exercise of authority. Or in a related formulation, the Court has stated that a delegation is permissible if Congress has made clear to the delegee "the general policy" he must pursue and the "boundaries of [his] authority."[34]

A policy of unconstrained disclosure mandates, as I've tried to articulate above, probably falls afoul of either of these formulations.

Justice Gorsuch, who disagrees with the "intelligible principles" 'test,' articulated in his dissent several reasons why it is a *good practice* for Congress to retain its legislative power instead of giving it to executive branch agencies. Among others:

> Without the involvement of representatives from across the country or the demands of bicameralism and presentment, legislation would risk becoming nothing more than the will of the current President. And if laws could be simply declared by a single person, they would not be few in number, the product of widespread social consensus, likely to protect minority interests, or apt to provide stability and fair notice.[35]

I think each of us, no matter our ideology or political preferences, can think of a president serving in our lifetimes to whom we would not want to give broad power to force disclosure from platforms. We would not want his administration's allies investigating given segments of the society and their behaviors. Legislation that provides unlimited support for transparency in the form of an unconstrained platform disclosure mandate seems to be an unwise idea, which may soon fall afoul of constitutional limits.

Should my concerns about overbreadth be at all persuasive, there are aspects of platform transparency that I recommend explicitly restricting as a start. Making platform moderation strategies transparent threatens to undercut those strategies. Transparency should not make the social media experience harder to oversee for the companies and worse for consumers. The same logic applies to security.

Do Not Mandate Disclosure of Moderation Strategies or Tactics

One of the leading thought pieces on how social media could be done better is "Protocols, Not Platforms: A Technological Approach to Free Speech,"[36] an August 2019 piece by Mike Masnick, editor of the prolific, long-running TechDirt blog. His brief is that we have seen a shift from widespread use of

common protocols, such as the email protocol (i.e., SMTP), to platforms such as Facebook and Twitter. This is partly because platforms can curate the user experience better than users grappling with technical protocols themselves. Given revenue sources such as advertising, platforms have an incentive to maintain themselves in the way protocols do not.

Masnick argues for a shift back to protocols, dangling the possibility that integrating crytpocurrencies into protocols might create revenue sources that support maintenance of protocols as such. This could supplant the need for targeted advertising, with its privacy costs for people concerned about commodification. More importantly for our purposes here, it could move editorial decisions, including moderation decisions, back to the edge of the network—back to users themselves.

A shift so grand does not have to happen for things to be different. I have watched, bemused, as consensus has emerged among pretty much all elite segments (policymakers, journalists, platform leaders, and so on) that the platforms must moderate content for their users rather than giving users tools to moderate content themselves. (CDA 230 may have had some part in this.)

I noted above my government transparency website, WashingtonWatch.com. It enjoyed brief periods of attention. One bill to extend unemployment benefits, for example, received more than 200,000 comments from users who grouped themselves into warring factions. (That's, maybe, three minutes' worth of material on a major platform nowadays.) Supporters and opponents of the Ethiopian government clashed on my site. Some alleged to me that users of my site had dishonestly adopted their identities to misrepresent their positions on Ethiopian politics.

Committed to free speech, leery of personally moderating all that content, and having zero budget for staff, I built rudimentary tools for self-moderation. WashingtonWatch.com allowed people to block the words of their choosing, other speakers, and so on. I did intervene when pure scatological content was posted, when a clear violation of someone's legal rights occurred, and in one instance when someone posted a federal elected official's private cell phone number. (I could not adjudicate claims of Ethiopian identity fraud.)

This hardly makes me an expert in platform moderation, and the problems I encountered were modest compared to what the large platforms see. What I observed, though, was that some users were relentless in their efforts to reverse engineer and then evade every moderation policy and practice. Given automated word-based moderation, they would vary words and spellings. They recognized the hours of the day that I was active, and they posted obnoxious content when I was "off the clock."

It was fascinating to see the herculean effort that went into defeating a small website's attempt to create a functional, debate-oriented community. I was not the most sophisticated webmaster, and I do not know whether I was confronted by a few extremely dedicated individuals or groups of collaborators. Whatever the case, I recognize from my experience that content moderation is extremely difficult, a fraught, spy vs. spy–type challenge. Broad strategies and narrow tactics are probed and tested relentlessly by those trying to turn social media platforms to their own advantage—or just trying to ruin them.

The concept of the "attack surface" in computer security is a helpful metaphor. A simple computing system that integrates with few other systems has a small attack surface because it has fewer vulnerabilities. A complex, highly interactive system will have exposure to many more vulnerabilities and thus a larger attack surface.

Think of platforms' moderation systems as a having an attack surface to protect. It is easy to see how forced disclosure of data about those systems would increase the attack surface. Once a university-affiliated researcher has a line into data related to a platform's moderation system, the attack surface is not just the platform's systems. It now includes the communications links to the researcher, the university's computing infrastructure, the researcher's personal computing and communications tools, and any student-assistants' computers and communications. The PATA bill addresses this risk to a degree by requiring the creation of security protocols, but the creation of risk here is ineluctable. One can predict that those security and privacy protocols will fail at times, with greater or lesser consequences.

The better way to secure systems is to leave their attack surfaces smaller. I recommend excluding moderation systems in statutory language from the forced transparency regime.

I make the same recommendation as to platform security, both measures taken to secure the platforms themselves and the measures platforms take to provide security to users. Statutory language should specify that no data from or about security systems should be subject to mandated disclosure. The risks disclosure would create seem more likely and greater than the diffuse, contingent benefits of a disclosure mandate.

We are still in a time when responsibility for data breaches and security failures is hard to pin down. If disclosure is mandated around platform security, that will create a diffusion of responsibility. When breaches and losses occur, the platforms, researchers, and universities involved may all point fingers at each other. My preference would be for the one responsible party, the platform, to be on the hook for

whatever wrongs and harms occur.

Here I have suggested carving out information and data related to moderation and security from any disclosure mandate. The same principle applies with respect to the personal and private information of users, which I treated at length above, focusing on the property rights that should protect them. I do not see the privacy-versus-transparency trade-off offered by PATA as a good one.

At some risk of "constitutionalizing" every issue, I will now turn to the First Amendment values that are threatened by mandated platform transparency, even if you accept my advice to exclude moderation data, security data, and personal data from your transparency ambit.

Mandating Platform Transparency Impinges on Free Speech

In case it needs saying, the object of your transparency efforts are platforms for speech and communication. Below, I will briefly articulate how I see speech as a direct object of the mandated disclosure in the PATA bill. Perhaps lacking in breadth of vision, I see general transparency mandates placed on in any industry as anomalous. It would be even more strange and difficult to mandate transparency on constitutionally protected speakers. I begin with a brief exploration of our interest in "algorithms."

When your computer pings a server asking for a given web page, an algorithm determines exactly what content the server returns based on things like the type of browser you are using and the screen resolution of your device. When you search on Google Maps for a store, an algorithm might include in your result that the store is open or closed based on its hours and the current time of day. That algorithm is a little more interesting, but it is nothing like the algorithms that the PATA bill seeks in the name of platform transparency.

The bill is (ahem) transparent about what algorithms are interesting. Section 12(g)(1) defines "algorithm" as a computational process with a "purpose of determining the order or manner that a set of information is provided, recommended to, or withheld from a user of a platform, including the provision of commercial content, the display of social media posts, recommendations of user or group accounts to follow or associate with, or any other method of automated decision making, content selection, or content amplification." I would summarize that definition as "automated editorial choices." Section 12 authorizes the FTC to require platforms to disclose their automated editorial choices.

I will draw again on my Fourth Amendment knowledge to reach what is really a First Amendment point. There are a small number of industries so closely regulated that they are treated as not having a Fourth

Amendment right against inspections without a warrant. These are liquor sales,[37] firearms dealing,[38] mining,[39] and running an automobile junkyard.[40] Each either has a present or historical association with crime, or physical danger is a manifest element of its operations.[41]

In *City of Los Angeles v. Patel*,[42] the Supreme Court invalidated a statute requiring hotel operators to make their registries available to the police on demand. The Court brushed aside the argument that hotels are so closely regulated that they lack the rights that apply generally to individuals and businesses. The requirement struck down in *Patel* is the closest analogy I can think of to the general warrant requirement that PATA authorizes. Section 12 gives the FTC power to require that platforms should report to the government in detail on their editorial choices.

A general order to disclose business practices and records would fall afoul of the law for all but the small group of exceptional business lines noted above. But platforms are businesses whose stock in trade is speech. The Internet and social media are strange but real descendants of the printing press, disembodied and given to everyone to use as much as they want. Social media companies aggregate and augment this mass exercise of expression. Given the communicative dimension of these services and the First Amendment's brusque tone in saying "Congress shall make no law … abridging the freedom of speech, or of the press….", I do not believe platforms fit in the category of "closely regulated" industries "long subject to close supervision and inspection"[43] that can be divested of their rights for purposes like crime control and worker safety.

There is an argument that platforms are so important and dangerous that they should be treated the way traditional fonts of crime and danger are. That argument could be availing if there were a tight means-ends nexus between accessing platform data and fixing the pathologies for which they are blamed. Close monitoring of auto dismantlers makes it much harder for them to operate as fencing operations. But platform transparency offers little in the way of concrete benefits or protections. It would be nice, but I do not think honest social scientists can promise concrete results of the type that justify government-mandated disclosure in the areas where it exists.

For me, it is even hard to lay Brandeis's "social and industrial diseases" at the feet of platforms. Their nature as communications platforms intervenes. Any harm or pathology that social media arguably produce or contribute to has a responsible actor: the social media user. A point I often make casually is that social media holds a mirror up to society, and people don't like what they see. One may blame the mirror, but more productive change may come from examining more deeply the roots of the many problems that social media seem to expose.

That may seem like a cold approach, inured against risks to democracy or the struggles that young people face online. But the urgency that sincere researchers feel about these problems does not imply their capacity to devise solutions. It may be that the personal, family, and community responsibility is what gets us through these challenges. I welcome orthodox university research as one part of finding solutions, but it is as likely that we collectively absorb what the new media environment means and develop strategies en masse for getting what is good from social media while mitigating their ill effects.

I do not share the premise that private, competitive communications platforms are a public resource through which researchers and government can tune society. That notion is at odds with our traditions, better judgment, and probably also the First Amendment. In these "hard" social times, I believe resorting to first principles will still serve us.

Transparency Done the Right Way

The demerits I see in mandated disclosure do not undercut the need for, or the value of, research into the new social media environment and its effects on all our health, interests, and values. We should have such research. So how do we get there?

Most of my experience with working to generate transparency is in the government sector. In a democracy the public's entitlement to transparency is something of a given. The private sector is different.

In case it needs arguing, social media platforms are on the private side of the private/government line. Yes, they exercise substantial dominion over the digital "spaces" they control, but the spaces they control are metaphorical. One exits these spaces by clicking on a link, turning one's eyes away from one's phone, or doffing the virtual-reality headset. If one must forgo interacting with one's peers to do so, that seems to be as much an exercise of communities' collective power (and inertia) than any platform's power to keep them there.

Governments control physical spaces, which are much harder to leave, practically and sometimes legally. Good governments assert a monopoly on the use of force within their jurisdictions to provide inhabitants of those jurisdictions security against wrongdoers and invaders. No platform ever detains, arrests, or jails a user. No platform ever goes to war against another platform. These are distinct entity-types: platforms are not governments. Platforms exercise some of the same authority over their "spaces" (again in scare quotes because they're metaphorical) as I do over my home. You have to follow certain rules while you're there, and you can easily leave.

Broadly, I see transparency in the private sector as any other good. It is a product of market demand.

As a thought experiment, ask yourself why we do not have to ask merchants to be transparent about the prices they charge. That information is "of the essence" for almost any consumer transaction. Failing to be transparent about pricing will generally produce an avalanche of shunning that puts tight-lipped sellers out of business.

Most other dimensions of consumer interest seem to work the same way, if with less unanimity. There may be a literature that analyzes how businesses work to satisfy the information demands consumers place on them, but as a casual observer I can see businesses respond to many dimensions of consumer interest: recycled materials/recyclability, country of origin, organic content, low cost, ease of use, good treatment of workers, and so on. I see no reason why consumer demand cannot press platforms likewise to be good stewards of their communities in any sense that matters.

Consumer demand does not need to be entirely spontaneous. As sophisticated actors in Washington, D.C., we all know that interest-based organizations of every stripe press for broader public recognition of the things they think are important. From direct appeals to consumers, to planting news stories, to placing op-eds and magazine articles, advocates shape the society directly. Nothing excludes researchers and universities from participating in these processes. There's a healthy community of academics who place articles in the popular press alerting the public to the dangers of social media, which naturally presses platforms to improve.

The media tends to portray tech titans as omnicompetent. If they are, their failings to protect consumers can only be the product of mendacity and evil arrogance. I suspect that the truth is a little less attractive and less black-and-white. Some of our social media and technology leaders are probably in way over their heads, overwhelmed by the enormity of what they have created and racing just to keep up. If they were in control, they would almost certainly ally with researchers to understand better the social and political consequences of their platforms. This is not to deny the profit motive, but the ESG movement (economic, social, governance) shows that corporations of all stripes can be brought to heel and pressed to do good while they do well, if that's what their customers want from them.

It may be obvious that the dynamics of social change in private markets is an interest of mine, but not my expertise. My ignorance particularly extends to the question whether the community of researchers wanting access to platform data has exhausted the approach of seeking partnership with platforms. The record that supports mandated disclosure would be incomplete if it is not shown that voluntary collaboration sought for a lengthy period has entirely failed. From what I know, mandated disclosure is a

cudgel that has not yet been justified by years-long, knowing intransigence on the part of platform leaders.

Moving back toward my potential strengths, I will offer a couple of policy prescriptions that I believe can support the market-driven research environment that I would prefer. As noted earlier, I might recommend modifying the CFAA to ensure that it addresses only true criminal behavior and does so proportionately. My sense as a non-expert is that it may criminalize behaviors that are properly treated as civil wrongs, and it may treat as wrongs things that are not wrong. If it indeed has draconian penalties, they should be reined in.

Privacy laws like those seen in Europe and California may be a substantial impediment to platforms' collaboration with researchers. The General Data Protection Regulation in Europe and the California Consumer Privacy Act are characterized by heavy prescription about what platforms (and others) can and cannot do with data. Our common-law system, by contrast, is generally harm-based. It does not list what can and cannot be done. It allows anything to be done provided that someone who harms another must make them whole. Under a harm-based system like ours, platforms have much more room to ally with university researchers and others to jointly explore the manifold effects of social media on society.

One option that seems almost radical is to ask consumers themselves if they want to participate in research. The question of platform transparency has a characteristic that you see in privacy debates sometimes, too. Government entities, advocates, and big companies debate about these consumer interests, treating actual consumers as an afterthought. If data about users is their property because of contractual commitments, as I believe, it should be harder to leave them out of the conversation. If social media users are to be the subject of research, perhaps they could be asked by a willing platform if they want to participate.

Notes

[1] Platform Accountability and Transparency Act, 117th Congress, 1st sess. (2021), https://www.coons.senate.gov/imo/media/doc/text_pata_117.pdf.

[2] See Jim Harper, *Privacy and the Four Categories of Information Technology*, American Enterprise Institute, May 26, 2020, https://www.aei.org/research-products/report/privacy-and-the-four-categories-of-information-technology/.

[3] See Jim Harper, "What Do People Mean by 'Privacy,' and How Do They Prioritize Among Privacy Values? Preliminary Results," American Enterprise Institute, March 18, 2022, https://www.aei.org/research-products/report/what-do-people-mean-by-privacy-and-how-do-they-prioritize-among-privacy-values-preliminary-results/.

[4] Jim Harper, "Understanding Privacy—and the Real Threats to It," Cato Institute, *Public Analysis* 520, August 4, 2004, https://www.cato.org/policy-analysis/understanding-privacy-real-threats-it#

[5] See, for example, Jim Harper and Neil Chilson, *The Semantics of "Surveillance Capitalism": Much Ado About*

Something, American Enterprise Institute, December 1, 2021, https://www.aei.org/research-products/report/the-semantics-of-surveillance-capitalism-much-ado-about-something/; and Jim Harper, "On the Cedar Point Nursery Decision: Now Do Intangibles," American Enterprise Institute, June 30, 2021, https://www.aei.org/technology-and-innovation/on-the-cedar-point-nursery-decision-now-do-intangibles/.

[6] "US Supreme Court Review of Petition for Writ of Certiorari in *Timothy Ivory Carpenter v. United States of America*," No. 16-402, August 11, 2017, https://www.cato.org/sites/cato.org/files/pubs/pdf/carpenter-v-united-states_1.pdf; and "Brief for the Cato Institute as Amicus Curiae Supporting Petitioners at *Timothy Ivory Carpenter v. United States of America*," No. 16-402, October 28, 2016, https://www.cato.org/sites/cato.org/files/pubs/pdf/carpenter-v-united-states.pdf.

[7] See, for example, *Symposium: Cyberspace and Privacy: A New Legal Paradigm?*, *Stanford Law Review* 52, no. 5 (May 2000), https://www.jstor.org/stable/i252780.

[8] Tony Honoré, *Making Law Bind: Essays Legal and Philosophical* (New York: Oxford University Press, 1987), 161, 162.

[9] Oren Bar-Gill, Omri Ben-Shahar, and Florencia Marotta-Wurgler, "Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts," *University of Chicago Law Review* 84, no. 1 (Winter 2017): 7–35, https://chicagounbound.uchicago.edu/uclrev/vol84/iss1/2/. But see also Gregory Klass, "Empiricism and Privacy Policies in the Restatement of Consumer Contract Law," *Yale Journal on Regulation* 36, no. 1 (Winter 2019): 45–115, https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3005&context=facpub.

[10] *Carpenter v. United States*, 484 US 19 (1987).

[11] *Carpenter*, 484 US at 26.

[12] Carpenter v. United States, 585 US (2018) at 14 (Justice Neil Gorsuch's slip opinion).

[13] *Riley v. California*, 573 US 373 (2014) at 2473, 2492.

[14] See Jim Harper, "Perspectives on Property Rights in Data," American Enterprise Institute, August 8, 2019, https://www.aei.org/technology-and-innovation/perspectives-on-property-rights-in-data/.

[15] In medieval times, ordinary possessions were "not esteemed of so high a nature, nor paid so much regard to by the law, as things that are in their nature more permanent and *immoveable*, as land and houses, and the profits issuing thereout." Travel and commerce necessitated putting personality "in a light nearly, if not quite, equal to . . . realty." William Blackstone, *Commentaries on the Law of England in Four Books, Vol. I* (Oxford, UK: Clarendon Press, 1765). Richard Pipes states,

> Sometime during the period in European history vaguely labeled 'early modern,' there occurred a major break in the attitude toward property. It was the consequence of the remarkable expansion of commerce which began in the late Middle Ages and accelerated following the discovery of the New World.

Richard Pipes, *Property and Freedom* (New York: Alfred A. Knopf, 1999), 25. Eric Jones examines theories that might explain how personal property rights took hold. Eric Jones, *The European Miracle: Environments, Economies and Geopolitics in the History of Europe and Asia*, 3rd. ed. (Cambridge, UK: Cambridge University Press, 2003).

[16] Since at least 2007, I have lamented the "cloud" metaphor for online services because it distorts expectations by eliding the complex of service providers and the protective obligations they have to consumers. See Jim Harper, "Good Stuff from Google / The Internet Is Not a Cloud!," The Technology Liberation Front, August 9, 2007, https://techliberation.com/2007/08/09/good-stuff-from-google-the-internet-is-not-a-cloud/; Jim Harper, "I Hate 'Cloud Computing,'" The Technology Liberation Front, February 6, 2009, https://techliberation.com/2009/02/06/i-hate-cloud-computing/; and Jim Harper, "Dropbox: A Privacy Black Box," The Technology Liberation Front, December 12, 2009, https://techliberation.com/2009/12/12/dropbox-a-privacy-black-box/. Given the time frames involved, it is appropriate to admit that I have been like Abe Simpson, shaking my fist at the cloud. See Know Your Meme, "Old Man Yells at Cloud," https://knowyourmeme.com/memes/old-man-yells-at-cloud.

[17] It is gratifying to see the judge-made doctrine of "qualified immunity" for government agents who harm citizens come under scrutiny and criticism in recent years. David Deerson, "The Cause Against Qualified Immunity," *National Review*, July 13, 2020, https://www.nationalreview.com/bench-memos/the-case-against-qualified-immunity/.

[18] Platform Accountability and Transparency Act, 117th Congress, section 11(a)(2).

[19] Jim Harper, "Remember the Common Law," Cato Institute, March/April 2016, https://www.cato.org/policy-

report/march/april-2016/remember-common-law#.

[20] Louis D. Brandeis, "What Publicity Can Do," *Harper's Weekly*, December 20, 1913, https://www.sechistorical.org/collection/papers/1910/1913_12_20_What_Publicity_Ca.pdf.

[21] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1980): 193–220, https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

[22] Sunlight Foundation, "Brandeis and the History of Transparency," May 26, 2009, https://sunlightfoundation.com/2009/05/26/brandeis-and-the-history-of-transparency/.

[23] See Alisdair S. Roberts, "Where Brandeis Got 'Sunlight Is the Best Policy,'" March 1, 2015, https://aroberts.us/2015/03/01/where-brandeis-got-sunlight-is-the-best-disinfectant/. Other antecedents of Louis Brandeis's notable quote can be found at Quote Investigator, "Sunlight Is the Best Disinfectant," https://quoteinvestigator.com/2020/09/22/sunlight/.

[24] James Bryce, *The American Commonwealth* (1888): 355.

[25] Mark Tapscott, "Watchdog: Cato Institute's Jim Harper Is on a Quest as a Digital Diogenes," *Washington Examiner*, December 19, 2012, https://www.washingtonexaminer.com/watchdog-cato-institutes-jim-harper-is-on-a-quest-as-a-digital-diogenes.

[26] See Cato Institute, "Deepbills Project," https://www.cato.org/resources/data; and Jim Harper, "Cato's 'Deepbills' Project Advances Government Transparecny," Cato Institute, May 21, 2013, https://www.cato.org/blog/catos-deepbills-project-advances-government-transparency.

[27] See Jim Harper, "Appropriate Appropriations? Transparency and Spending Control," Cato Institute, January 23, 2o14, https://www.cato.org/blog/appropriate-appropriations-transparency-spending-control.

[28] GovTrack.us, website, https://www.govtrack.us/. A worthy history of the effort to pull data out of the government can be found at Joshua Tauberer, "GovTrack Now Actually Uses Open Government Data," Medium, July 6, 2016, https://medium.com/civic-tech-thoughts-from-joshdata/govtrack-now-actually-uses-open-government-data-5fc16f377e86#.iflkyrvgs.

[29] Lily Ledbetter Fair Pay Act of 2009, Pub. L. 111-2, https://www.congress.gov/bill/111th-congress/senate-bill/181/actions.

[30] Angie Drobnic Holan, "Obama Breaks Promise on 'Sunlight Before Signing,'" Politifact, January 29, 2009, https://www.politifact.com/article/2009/jan/29/obama-first-broken-promise/.

[31] In 2011, I wrote about the data publication practices that would support government transparency, using water as a metaphor. Information and data must be potable, and it must be sought out by the public. Curiously, I did not use the line, "You can lead a horse to water . . ." See Jim Harper, "Publication Practices for Transparent Government," Cato Institute, September 23, 2011, https://www.cato.org/sites/cato.org/files/pubs/pdf/bp121.pdf.

[32] Chris Coons, "Coons, Portman, Klobuchar Announce Legislation to Ensure Transparency at Social Media Platforms," press release, December 9, 2021, https://www.coons.senate.gov/news/press-releases/coons-portman-klobuchar-announce-legislation-to-ensure-transparency-at-social-media-platforms.

[33] *Texas v. Commissioner of Internal Revenue*, 596 US (2022), https://www.supremecourt.gov/opinions/21pdf/21-379_c07d.pdf.

[34] *Texas*, 596 US.

[35] *Texas*, 596 US. (See Justice Gorsuch's dissenting opinion.)

[36] Mike Masnick, "Protocols, Not Platforms: A Technological Approach to Free Speech," Columbia University, Knight First Amendment Institute, August 21, 2019, https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech.

[37] *Colonnade Catering Corp. v. United States*, 397 U. S. 72 (1970).

[38] *United States v. Biswell*, 406 US 311, 311–312 (1972).

[39] *Donovan v. Dewey*, 452 US 594 (1981).

[40] *New York v. Burger*, 482 US 691 (1987).

[41] *See New York*, 482 US at 709 ("Automobile junkyards and vehicle dismantlers provide the major market for stolen vehicles and vehicle parts"); and *Donovan*, 452 US 594, 602 (1981) (describing the mining industry as "among the most hazardous in the country").

[42] City of Los Angeles v. Naranjihabai Patel, 576 US (2015), https://scholar.google.com/scholar_case?case=9421617728115309l9&hl=en&as_sdt=6,30

[43] *Colonnade Catering Corp. v. United States*, 397 US 72, 74, 77 (1970).