



Transcript

Transparency and the Tech Sector Conference

November 04, 2022

Contents

Panel: Why Transparency?.....	2
Keynote: Julia Angwin	31
Panel: The Shapes of Transparency.....	53
Panel: Transparency's Tradeoffs	78
Keynote: CO Senator Robert Rodriguez.....	105

Published February 14, 2023

Panel: Why Transparency?

[00:00:00.50] MARGOT KAMINSKI: So welcome to Transparency and the Tech Sector. I'm going to give a brief introduction right now about why this focus on transparency, and I'll do it through the lens of three stories, each of which shows the roles that transparency is expected to play and does play in the regulation of platform and information technologies. Hopefully, these stories will outline a set of questions about transparency that will follow through today. It shapes, its limitations, and its relationship to power.

[00:00:31.71] The first story is about content moderation and a company some of you might have heard of, called Twitter. Twitter was founded in 2006. And I'm sure, as we will hear about extensively today, it was founded into a particular regulatory backdrop in the United States of 47 USC Section 230, also referred to as CDA 230. Hi, Eric, the resident expert on CDA 230. Which immunizes internet platforms from liability for most user content.

[00:01:02.31] CDA 230 also importantly permits platforms to adopt their own policies for content moderation, immunizing them from liability for most takedowns of user content. Six years later after it was founded in 2012, Twitter began, like many of the bigger internet platforms, to publish a series of transparency reports. This included reports outlining its content moderation practices, even though it was not legally required to do so.

[00:01:31.48] The reports include data on legal requests made through court systems and data on enforcement of Twitter's rules in terms of service. From 2012 to the present, Twitter published these reports biannually. The original reports then evolved into a more comprehensive and interactive transparency center, which you can still go to and play around on, and I suggest you do before it potentially disappears.

[00:01:55.54] In 2016, Twitter convened the Twitter Trust and Safety Council, a group of now roughly 100 independent expert organizations from around the world gathered not so much to perform oversight over content moderation, but to advocate and advise Twitter on the development of its products and its ideas.

[00:02:13.63] Then Elon Musk took over last week. He fired Twitter's top executives, including the policy executive responsible for communicating with the External Trust and Safety Council. He has stated that he wants to form his own content moderation council with, quote, widely diverse viewpoints. And in the meantime, Bloomberg reported that there was a 1,700% spike in hateful conduct on Twitter on Saturday.

[00:02:38.62] So why do we care. Why, in particular, do we care about transparency? What role are these voluntary transparency reports, or now really a transparency center, playing in this otherwise permissive

regulatory environment? Were they serving the role well? Were they working? And what will be lost if Twitter no longer continues to voluntarily provide them going forward? What will be lost if Twitter decides not to interface in any other ways, including providing other forms of transparency to a wide range of stakeholders, including NGOs and researchers?

[00:03:14.20] My second story is more from the space that I play in and also, probably thankfully for you, shorter. This one comes out of data privacy. In 1973, the Department of Health Education and Welfare published an influential report on records, computers, and the rights of citizens. You heard right. That was 1973. The report considered the rise of computer-based recordkeeping and the risks that an imbalance of power would arise between those holding computerized records and those whose information is in those records.

[00:03:45.73] It is surprising, indeed almost shocking, just how relevant the 1973 HEW Reports analysis is today. It discusses the ways in which individuals might be trapped and frozen by their data as stereotypes. It discusses the way that data errors can travel and harm individuals. And the way that information gathered and analyzed in one context may cause harm when used in new contexts.

[00:04:09.40] Many of the report's substantive policy recommendations were about, you guessed it, transparency. In fact, the HEW Report developed what are now known as the Fair Information Practice Principles or FIPS, which are recommendations that now form the basis of data privacy laws around the world. At its core, the FIPS include the requirement that there shall be no secret records. An individual must receive notice that records exist, notice of how they're used, and be able to access what information in government agency or private entity hold about them.

[00:04:44.92] In practice, the implementation of these 1973 principles ranged a lot. From the heavily critiqued and largely characterized as weak notice and choice model that long governed in the United States, to the backbone of the European Union's General Data Protection Regulation, to our very own, and I'm very proud of this, Colorado Privacy Act and subsequent interpreting regulations.

[00:05:09.24] Essential debate now in privacy law circles is, again, why transparency? What is the aim of these different notice and disclosure rights? Is it to enable individuals to exercise other rights? Is it to check the power of the record keepers through market sanctions or other forms of shaming? Is this transparency working in this space? And for many people, the answer is a resounding no. We receive notices all the time. We rarely have time to make substantive choices. And if other tools are necessary, what tools should they be? What tools might be better?

[00:05:42.39] Finally, my third story comes from the realm of algorithmic accountability, otherwise known as the Law of Automated

Decision-Making or the Law of Artificial Intelligence. And I draw this example from the Electronic Privacy Information Center, EPIC's report earlier this year on the use of automated decision making by government in DC.

[00:06:03.10] Since 2012, the DC Pretrial Services Agency or PSA has used a pretrial risk assessment instrument, which is a computer program. The program's developers claim that given an input of 70 attributes, ranging from criminal history to race, it will predict a defendant's likelihood to re-offend before trial and fail to appear at trial.

[00:06:26.74] Across the country, courts use similar systems to determine both sentences and set bail. And you might have a moment where you say, well, this is about transparency in the tech sector. Why are you talking about government use of these algorithms? First of all, government procures these algorithms from the private sector, which itself uses various legal instruments to try to obscure the information on which they were developed, such as trade secrets. And second, one of our keynotes today, Julia Angwin, did a widely lauded report for ProPublica in which she used public records laws to get access to information about these private sector developed algorithms.

[00:07:03.73] So back to the problem. The problem is that the information that's entered into the algorithm to predict the likelihood of reoffense or failure to appear at trial itself reflects social facts. It reflects past policing behavior. That is it reflects police decisions to stop, search, and arrest people, or let them go, which themselves reflects longstanding biases and practices of discrimination.

[00:07:27.73] According to EPIC's report, there is some good news. After the ProPublica report, these recidivism risk algorithms were largely critiqued. And this particular automated decision making instrument used in DC undergoes now periodic testing. It has been updated after independent review to place more emphasis on recent criminal charges and less emphasis on other proxy factors, such as likelihood of arrest.

[00:07:51.85] The system also underwent a validation study to try to test its actual efficacy in predicting re-offense and a predictive bias report. And even so, after all this oversight and transparency, the system was about 7% more likely to incorrectly identify Black defendants as high risk compared to White defendants. Evaluating a similar system or the use of a similar system by prosecutors, the Wisconsin Supreme Court found that there was no due process right to inspect the source code of the algorithm or otherwise, to challenge it and relied instead on a warning to judges not to rely on such instruments.

[00:08:29.17] So once again, what's the role of transparency here? What can and can't transparency do? How do technical limitations and legal limitations like trade secrecy or complex programming shape the

type of transparency that's made available? What's the difference between a systemic level of transparency, such as an audit, versus individualized transparency, such as a right to actually be told how a computer made a decision about you that significantly affects your life?

[00:08:57.20] So in closing, I want to briefly review what these three stories tee up for our conversations today. They suggest that there is significant value to transparency sometimes, even if Blake Reid in the back corner might disagree. They reveal systemic practices and impacts. They enable the shaming of companies and spur changes in behavior. Transparency can enable the public to deploy market forces as sanctions for companies that they dislike.

[00:09:24.09] Transparency can serve as a catalyst for policymaking by regulators. It can enable other individual rights, such as the right to challenge an automated decision making system, which is impossible if you don't know how the decision was made. And transparency can actually serve an oversight function over the regulators that are regulating the private companies as well, forcing them to be accountable to the public, rather than captured.

[00:09:46.92] These stories suggest too that transparency is far from uniform. Its settings are also far from uniform. It comes in different shapes and sizes, from access, to explanations, to voluntary annual reports, to audits, to oversight by third parties. It shows up across many different branches of technology law with wildly different enforcement mechanisms and sometimes, no enforcement mechanisms at all.

[00:10:11.71] And finally, to give some credit to Blake, these stories do suggest to limitations of transparency, that it can be a Band-Aid rather than a cure, that it can present as a first step to regulation that never ends up materializing, and that it could be in tension with other values, including privacy and data security. And finally, that relying on voluntary private sector transparency has significant limitations when billionaires buy major media platforms.

[00:10:39.45] Today, we'll proceed as follows. Our first panel here will discuss the why of transparency, the reasons for it and its goals, followed by a short break. Our first keynote will then be from Julia Angwin, founder of The Markup and winner of the Pulitzer Prize in journalism. She'll be joining us virtually. Then lunch will be provided.

[00:10:59.22] And our second panel will discuss the many forms transparency can take, and what works, and what doesn't. Our third panel will discuss transparency's tradeoffs, what is lost if everything is transparent. And finally, our second keynote will be from Senator Robert Rodriguez, Senator of the Colorado Senate District 32, a prime sponsor of our very own Colorado Privacy Act. I want to note just in conclusion that our proud tradition here at Silicon Flatirons is to begin each question and answer session with a student question. I hope you will all enjoy today, and I look forward very much to our discussions to come.

[00:11:41.28] DAVID SULLIVAN: So thank you, Margot, for that really incredibly thought-provoking introduction, which I think is going to shape this panel's discussion and the rest of the day. My name is David Sullivan. I'm the executive director of the Digital Trust and Safety Partnership, which is a partnership of technology companies working together to articulate best practices for trust and safety.

[00:12:04.34] Transparency is one of the five sort of core commitments that our company members make. I'm also on the Silicon Flatirons advisory board. And I am thrilled to be moderating this discussion with some of my favorite people and some of the sharpest thinkers in the tech space. So I'm going to introduce them very briefly, so we can spend as much possible time in discussion and also have that time for Q&A and bringing the expertise of the folks in the room into the conversation. So

[00:12:34.70] From right to left, starting here. So we have Bri Riggio, who is platform policy manager at Discord. We're going to talk a little bit about what that actually means. And to her left, we have Daphne Keller, who directs the program on platform regulation at the Stanford Cyber Policy Center. Did I get that right? Then Evelyn Douek, assistant professor at Stanford Law School. And finally, and last but not least, Alex Walden, who's the global head of human rights at Google.

[00:13:16.02] So I'm going to be posing questions to each of our panelists. But after they give their initial remarks, it'll be opened up for others to weigh in as well. And I think with that format, we're going to try to have a really free-flowing conversation and just try to hit as much as we can on this panel's topic, which is why transparency? Which oftentimes I think is a question that whether you are a policymaker or regulator and someone from an NGO, someone from a company, maybe doesn't get asked as early enough in the process of thinking about these issues as it should be.

[00:13:54.87] And so on that note, we're going to start with Evelyn. And so the question really is what role should transparency play when it comes to particularly content moderation and regulation of content and content laws?

[00:14:13.37] EVELYN DOUEK: Well, thank you, and thank you everyone for the opportunity to be here and in organizing this conference. I think it's a fantastic program. I'm looking forward to learning from all of you today. I think this is a great and really important, and as you said, often overlooked question that we could probably spend the whole day answering, which is why transparency? And it is so centrally important because transparency is an instrumental good. It is not an intrinsic good.

[00:14:38.57] You only want transparency in order to achieve some other aim. And so the why you're asking for it will inform the what you're asking for, as well as from whom and to whom. And every single one of those is a variable and informs lots of different kinds of

transparency that we might want. There is no such thing as transparency as a monolith, and there's also no such thing as accountability as a monolith.

[00:15:09.33] And so every single one of those things needs to be broken down. And it's not that there is a best form of transparency. I think there's multiple forms of transparency that we would want for multiple different purposes. And without being specific about, it we run the risk of doing exactly what Margaret was talking about, about getting sort of transparency theater or transparency that doesn't achieve anything. We can be drowned in transparency with actually learning very, very little.

[00:15:41.67] And I think some of the transparency that we already have has fallen into that bucket. If you look at some of the industry reports, not pointing any fingers, but industry reports that we get about mass numbers of takedowns of pieces of content falling into certain categories, it tells you so little about what's going on within that system. It doesn't tell you were those decisions are accurate? It doesn't tell you how many times was hate speech missed and not taken down?

[00:16:08.78] It doesn't tell you why is that number increasing? Is it increasing because the platform is getting better at finding hate speech? Or is it increasing because there's more hate speech on the platform, and actually, the platform's getting worse at detecting it, and the numbers that they're missing are getting bigger? And I could keep going on, but we're getting these reports that maybe progress, and it's great. I really appreciate the industry opening up and giving us some. Data but without being really specific about what you want, we run the risk of wasting everyone's time because I'm sure a lot of time and energy goes into that within the companies as well.

[00:16:45.28] So we can talk a little bit about some of the forms that might be useful and to whom, from whom. So platforms to users can be a really important form of transparency. And users, by the way, are not the ones reading those transparency reports. Like 50% of the people reading transparency reports are probably in the room right now. It is not the one billion users that are reading how many pieces of hate speech Facebook took down last quarter.

[00:17:14.40] But there are really important forms of transparency, including notice through the kinds of rules that the platform has, to tell them what they can and cannot do. Telling them why a piece of content violated the rules. In many cases, platforms have released some data that shows if you tell them. Most people are not bad actors they want to reform their behavior, and they will try and do better in the future.

[00:17:33.58] And so all of those kinds of transparency, and there's important work from Tom Tyler in Yale and his research group that shows that increases the perceived legitimacy of the decision making, even when a user has a decision go against them or even where they

disagree with the decision. The fact that they know what's going on, they know why the decision was made, that increases their trust.

[00:17:55.83] We also might think about other institutional actors who it enables counter speech. So if we know a bit about what's going on the platform, if we know the kinds of disinformation, if we know the kinds of things that they're seeing-- free speech tradition really believes in counter speech. And so if we have election disinformation, election officials can, for example, say no, no, this is the voting time. Or no, no, this is how we do voting, or counting, or whatever it is, can be a really important way of doing that. So not censorship, but enabling counter speech.

[00:18:30.12] One of the most important forms of transparency is checking what the rules say on the books and on the websites match what platforms do in practice. And this is a big area of opacity at the moment, where the rule books for most major platforms these days look pretty good. It's hard to disagree with a lot of-- I mean, we will disagree, and we will argue around the edges. But by and large, this sort of well thought out, really thoughtful policies, we just don't know how they're being applied in practice.

[00:19:03.51] I think industry learning and industry standards can be a really important part of transparency. So I am also really nervous about what might happen with Twitter because Twitter has really led the industry on transparency. And one of the pieces of transparency that I love is they tell you how effective their interventions are.

[00:19:20.67] So for example, my favorite piece of content moderation trivia is that Twitter introduced this little pop-up where if you go to retweet an article that you haven't read, a little thing will pop up, and it'll say, hey, do you want to read this before you spread it further in the world? It's totally gentle. You can be like, no, I just love the headline. But you can say, OK, yeah, sure. And 40% more people, 40% more people clicked through and read the article, which says how simple creatures we are.

[00:19:51.82] But I also think that says to the rest of the industry, hey, have you thought about nudges? Nudges can be quite an effective tool in content moderation. And finally, I think avoiding abuse is an obvious reason for transparency. And here's where we might want transparency not just from platforms, but for example, from governments, about what they're doing when it comes to content moderation.

[00:20:14.43] How many requests are they making? What kind of requests are they making? Who are they making requests to about taking content down or getting data or things like that? And I think that's a really important one that all the transparency burden doesn't necessarily need to be put onto platforms, but can come from other actors, including civil society, like who are talking to, and what kind of input do you have?

[00:20:35.80] So I'll close by saying this is an iterative project, and we can't let the perfect be the enemy of the good. I think that we're never going to get one perfect transparency ask. We're not going to solve it today. And often, getting transparency only enables more questions and better questions. And you go, oh, that was really interesting. Can you tell me more? Which I'm sure can be really frustrating for people in industry because you open up your books, and then people like, you haven't told me this piece of information that I want to know.

[00:21:04.09] But I do think that keeping in mind that we don't need to get it perfect straight away, that we can keep working on in, keep improving, as long as we keep in mind that what our original goals are and not just sort of transparency for transparency's sake.

[00:21:20.71] DAVID SULLIVAN: Well said. Does anybody want to just jump in and add to or maybe try to subtract from that before we move down? So if not, I think that sort of perfectly tees up the kind of like a pragmatic approach to sort of why we want transparency. And I think then helps us lead into our speakers from companies.

[00:21:44.78] And so I wanted to start with Alex, head of human rights at Google. So from a human rights perspective, like what is the role of transparency in Google's human rights responsibilities, and what does that look like, especially in terms of the kind of public reporting aspect of transparency?

[00:22:05.24] ALEX WALDEN: Well, that's a great question. And again, thank you for inviting us to participate in the symposium today and on the session. I'll just start on a reflection I had this morning when I was thinking about this panel and thinking about. So I've been at Google now for about 7 and 1/2 years. And the conversation that we were having about transparency then, I think it's important to appreciate how much we've evolved in that time. And I folks like Daphne and others in this room have been working on it since before then.

[00:22:36.67] But even in that 7 and 1/2 years, there was sort of a conversation happening between a very small group of folks who work on digital rights. And now, it's a conversation-- those people are still having it and driving it in many ways, but it's a much more public conversation being had with governments, and the public, and other stakeholders in ways. But I think it took us a long time to get there. So I think that's sort of one important piece of thinking about why it's important for companies, but also how we've evolved our thinking about transparency over time too.

[00:23:08.35] So you know, like Google was the first company to launch a transparency report. We did that in 2010. And at that time, we were really focused on what is the relationship between governments and companies? And how do we make sure the people using our platform and the public generally who is also holding their governments accountable understands what the request look like that companies are getting from governments? What are they asking us to

do? What content are they asking us to take down? What data are they asking us to hand over? And so how can we make sure people know that, both to educate us in our use of platforms and also in our conversations with government.

[00:23:45.37] So that's sort of like really where it started for us, and that's very tied to the company's principles around human rights. And I think it sort of coincides with the beginning of organizations, like the Global Network Initiative, where companies were really coming together to try to understand the dynamic of what they were doing, and their relationship with the government, and how they could share more information about that to educate all stakeholder groups, so that we could just have a better conversation about how to come up with solutions.

[00:24:19.37] But just to your point, what is the primary reason we do this from companies? It's really about the trust of the people using our platform. We want people to understand how our platforms work and how they're engaging with it. And so I think it gets to a lot of the things Evelyn raised, which is about what kind of transparency. We're talking about a lot of different kinds.

[00:24:39.16] So I think, again, in the past, the conversation really focused on transparency reporting, which is still an essential part of this work. But really, we need to expand the way we think about this both qualitatively and quantitatively and then also the different kind of groups of people who need transparency.

[00:24:57.94] And so that's about our individual people who are using our platforms and how we engage with them, as you said, how we notify our users, and making sure that they understand why we're taking actions and what they can do to ensure that they're working within the bounds of our policies and vice versa, I guess.

[00:25:18.73] And then there's the general public. And I think that for everyone to understand how our policies work, the way that we're governing our platforms, that's both qualitative and quantitative. And then for regulators to understand from really a compliance perspective how are companies doing the things that they say they do. And transparency might look a little different in that way and might not always be public.

[00:25:41.38] And then I think the last category is really one that I think has finally gotten more traction in the past handful of years, and that's about researcher transparency. And so what does it look like for companies to protect the privacy of their users and sort of maintain fidelity to their terms of service and then also create opportunities for researchers to evaluate these questions. What are the trends that we're seeing, and how could we be doing better in our enforcement?

[00:26:09.77] So that's sort of the primary reason. It's really about user trust. But I do think, again, from a human rights perspective. The other

big piece is that just fundamentally, if you are a company who's committed to human rights, and lots of the large platforms are, it's sort of incumbent upon you to proffer transparency artifacts to enable the conversation among stakeholders. Companies that are committed to human rights are also committed to a multi-stakeholder conversation and recognize that solving problems in the online space, there's a role for everyone, for companies, for civil society, for researchers, and for government. And for us to enable that conversation, we have to be more transparent about it.

[00:26:52.70] So it's really sort of just table stakes if you are a company that cares about and is committed to human rights. And that's obviously going to be regulated for companies over time as well. But I think some of us have sort of understood that that was necessary from the beginning. I will stop there because I know that's a lot of fodder for us to talk about.

[00:27:13.03] DAVID SULLIVAN: It's perfect because I think we're starting to fill in some of the variables that Evelyn set out and talk with a little bit more specificity about what kind of transparency, to whom, from whom, et cetera. To that end, I want to go to Bri next, and to sort of transition from a more external-facing company perspective in terms of that human rights role and that multi-stakeholder conversation with external stakeholders, to break down what it means to be developing the rules for a platform. And what a platform policy manager does, and how that relates in particular to setting expectations about the rules and guidelines for a platform and the community of users of it.

[00:27:59.17] BRI RIGGIO: Yes, Thank you. Thank you for that question. And thank you to my lovely panelist as well who I feel like have teed me up very well to kind of answer this. So I'm going to answer this question or kind of get at this question of transparency from particularly a platform policy lens. That is the work that my team and I do, and that's how I'm usually thinking about transparency.

[00:28:19.94] So when I mean platform policy, what do I mean by that? I'm referring to the policies that we write or put together that basically underwrites our community guidelines. What is, or probably more accurately, what is not allowed on the platform? Some companies will refer to this as content policies. At Discord, we call them platform policies.

[00:28:40.72] And I want to talk a little bit about the benefits that can happen with transparency to users around these policies. So when I'm thinking about that, there's kind of two pieces to this. The first is really thinking about are our policies actually transparent to users kind of from the get go, from the ground up? Do our users understand what the policies are, where to find them, how to follow them?

[00:29:06.97] Those policies, assuming that users know what they are and are willing to follow them, can also really help set the norms, the expectations around what kind of activity, what types of posts are

actually appropriate for the platform? What are the norms of that platform in the communities you're participating in? So for instance, if we were to put out a policy that says no harassment at all, we have to define what that means for the users. But that does set the expectation, hey, don't go out of your way to harass people. Don't go be mean to people.

[00:29:37.24] The second layer to then is in the instance where users are violating policies or a user has violated a policy transparency around, hey, you violated the policy. What policy did you violate? What particular part of the policy potentially did you violate? And then what do you have to do to essentially get back into good standing?

[00:29:58.30] Assuming you're not completely banned from the platform, of course, how do we educate users? How do users know how to basically make sure they don't end up in that situation again? And part of this as well is all in service of safety of the platform, right? Safety of our users. Again, it's just another area to kind of set expectations and also build that trust with our users, which was mentioned just a bit ago. There's really that opportunity there when you are willing to be more transparent.

[00:30:26.89] There's also this other element too where I think it's important for other users who maybe haven't committed the violations and aren't receiving some kind of enforcement response to also see and to also understand how is this platform enforcing the policies? Are the policies actually being enforced? Again, it's another area where that trust is being built. It's another area where the policies actually mean something. We're not just saying something and then just letting it be kind of a free for all space. And so again, that element of transparency then continues to build the norms, continues to build the expectations, continues to build the trust.

[00:31:07.18] So I say all of this kind of with the understanding that not all users, most users actually when they're violating policies are not intending to do so. They're not necessarily doing it maliciously. They're doing it either because they didn't realize there was a policy there that they were violating, or maybe they posted something and just didn't realize actually that falls within the scope of a policy. And so again, that education piece comes in.

[00:31:32.65] There are, however, some actors who are doing it maliciously. Prior to jumping over to working on platform policy, I headed up Discord's counter-extremism team. So thinking about issues of countering violent extremism, countering terrorism. And in that space, we were frequently dealing with and talking as a team, how do we deal with adversarial actors?

[00:31:57.22] And so for those in the audience who, maybe this is the first time you're hearing this term, the idea of an adversarial actor is someone who for whatever reason is really dedicated to using your platform. It serves a purpose for them, and they want to use it at all

costs. A lot of the time, the actors who are engaging in this behavior are doing so from kind of a very high harm, high physical safety threat position. Think about issues, again, violent extremism, child safety.

[00:32:29.14] And the idea here is that they will evolve their efforts to basically circumvent your detection, circumvent the actions that you might take against them. And as you as a platform adapt your responses to be able to find these individuals, to remove them, to keep your platform safe, they will also evolve their tactics. And so that's where that adversarial perspective or that adversarial piece of it really comes in.

[00:32:57.26] And so when thinking about these actors, there is the potential that when you are being more transparent about how are you enforcing these policies, how are you detecting them, that by being transparent there, you potentially are giving the adversarial actors, these individuals who you want to take down, you are giving them information on how to better kind of evade you.

[00:33:19.81] I think there's kind of two minds of this as well. I mean, on one hand, certainly we could say, well, these actors are going to figure out. They're going to figure out this anyways. And so err on the side of transparency. There's so much more good to be coming from that. But at the same time, if there's an opportunity to not give that information out, then there's potentially a justification for doing so.

[00:33:41.05] And then finally, I'll wrap this up by saying that in those very highest harm or severe kind of situations where potentially we're dealing with maybe even illegal activity, and law enforcement is involved for whatever reason, there's also a potential drawback, a pretty significant potentially drawback to offering transparency to users engaging in this activity. And so in that way, transparency can really backfire.

[00:34:07.21] So for instance, we can think about a situation in kind of the child safety realm. Say we have an adult who is preying upon a child. Law enforcement is involved. If you were to tell that adult we've removed your account, or we've taken action here because we're aware of the behavior that you've been engaging in, that potentially tips off that user to go and potentially hide the activity that they've been doing, to go erase what may potentially be evidence in some kind of case.

[00:34:35.89] It may also encourage them to find another way to recontact the child and then try and kind of solidify control over the child or basically anticipate punitive action that might be coming even outside of the platform. So I will wrap up there. But just to say that I think in general, there's a lot of good that comes from transparency, particularly when platforms are thinking about building that trust with users, building the norms and the expectations of the platform and what you're trying to build. But counterintuitively, there are some situations where more transparency or transparency kind of at all costs

can actually backfire and actually make users more unsafe in certain situations.

[00:35:17.64] DAVID SULLIVAN: Thanks, Bri. I think in less than a half an hour, we've basically had a crash course in what does it mean to try to, one, build a healthy community and maintain a kind of trust between the company and its community of users and this wider set of stakeholders. I wish that more policymakers and regulators in different places around the world might have all of this information at hand. Sometimes, they do. Sometimes, they don't.

[00:35:44.72] And to that point, I want to turn to Daphne. The legal environment, both in the US and around the world when it comes to transparency and to content has been shifting dramatically. What are legislators and regulators trying to achieve with transparency, and what does that look like right now?

[00:36:05.76] DAPHNE KELLER: Well, I don't think they know. Nonetheless, they have enacted some laws. So there are some major new transparency laws either about to come into effect or already enacted but sort of staid right now. This includes the Digital Services Act in the EU. And the laws passed in Texas and Florida that are being litigated in the next phase cases have significant transparency provisions that are part of what's being challenged in that litigation.

[00:36:38.22] I'm going to try to, in this presentation, walk through briefly what the purposes might be of the transparency, what the countervailing interests might be, and how to balance them. And I'm deliriously tired. So if I pause slack-jawed and stare at my notes, that will be why.

[00:36:59.07] So when I first started talking about transparency in my role at Stanford, I thought of it primarily as a way to get governments better information that they could use in crafting better laws because we were seeing things like proposed laws saying, hey, platforms, take down all the bad things. And with better transparency, we would be able to illustrate how those kinds of laws can backfire through over broad removal and so forth.

[00:37:26.28] And in fact, because of the happenstance that there is transparency about that under the DMCA with this treasure trove of notices sitting in the lumen database at Harvard, so that independent researchers can analyze the question, we know that there is a major pattern of over-removal, which is the kind of thing that you would want governments to know when they're enacting laws for a platform regulation.

[00:37:53.21] I think that is not what the lawmakers in the DSA or Texas or Florida have in mind. I think that a lot of the transparency rules in there, at least in the EU or maybe the ones that the people in this room think about, have more to do with what I would think of as a Democratic self-governance interest, which is finding out if I, or my

neighbors, or my cousin in Wyoming, or whatever have been exposed to disinformation campaigns. Whether we are on the receiving end of content moderation by platforms that reinforces racial bias.

[00:38:29.55] There are all of these questions about our information ecosystem that we can't really manage our lives and politically participate unless we have better answers to those questions. And so I think that's what motivates a lot of things like the draft platform and Algorithmic Transparency Act in DC, which has things like research or access to data and freeing up researchers to scrape content.

[00:38:55.29] Then the third sort of state interest or goal that you might have is consumer protection for users to understand what it is that they're going to get before they decide to use a platform or know what the rules are. And a strange thing that's happening in the net choice case is consumer protection is the only interest being advanced by the states.

[00:39:20.96] So this whole question of whether there's a Democratic self-governance interest, and what kinds of rules that would justify, and whether that increases the state's interest or changes how you think about tailoring the laws is just absent from those cases, which is a very strange way to be coming at the question I think.

[00:39:38.90] So moving on to the countervailing interests. The first one I think is what Evelyn called wasting everyone's time. I think there is a real risk that transparency mandates will cause platforms to go out and do a whole lot more work than is actually useful for the people who are on the receiving end of the transparency.

[00:40:04.93] And if the platform we're talking about is YouTube or Facebook, maybe we don't care. Maybe our tolerance for making them do potentially unnecessary work is endless. But just to kind of look at the numbers, in NetChoice, YouTube said in its filings that right now, every quarter, it notifies nine million people about video removals and lets them appeal them. But if the Texas law forces them to also cover comments in the same way, that number will go up to a billion notices and potential appeals a quarter, which is a huge uptick.

[00:40:43.15] And if your opinion of YouTube comments is anything like mine, like I'm not sure that that's always the best use of resources. Again, maybe we're fine making YouTube do it. But the Texas and Florida laws make a bunch of smaller mid-sized companies do this, one of which, full disclosure, is Pinterest where I do some consulting. And the Digital Services Act in the EU has these mandates all the way down to platforms that have just 50 employees and that make 10 million euros a year.

[00:41:18.80] This I think is a dangerously anticompetitive setup, the idea that much smaller platforms will be forced to bear these big burdens far, far earlier in their development than the giant incumbents did is not a setup for actually having new market entrants come along

who will challenge those incumbents. So I am worried about the wasting time/competition problem.

[00:41:44.69] The second concern is privacy. And this is a question that really varies depending on which model of competition, which specific disclosure mandate you're talking about. But for example, a lot of conversations I'm in with people thinking about drafting transparency laws or drafting them, they don't necessarily the ways that aggregate data disclosures can actually be crunched down to become individual personally identifying information about the users.

[00:42:18.04] They are not conversant as the privacy people in the room may be with things like NetChoice releasing aggregate data and researchers being very swiftly able to identify individual users. So there's just like translation or education process I think that needs to happen, so that we don't accidentally wind up with laws that create that problem.

[00:42:40.37] There's also a question about laws like research or access mandates, like the ones in the DSA or potentially in PADA in the US. Are researchers going to get access to the actual content of people's communications, including private communications? Is that what we want? Are they just getting metadata? And is that what we want?

[00:43:09.53] And there's a legal issue there about surveillance and privacy, which is if platforms are handing over private information to researchers, does that information lose protections from state surveillance that it would have had under ECPA or would have had under the Fourth Amendment had the data stayed where it was with the platform? So there's just like a big question to sort out. And I hope we slow down in the US and sort out that question before enacting the laws.

[00:43:37.26] And I have to admit that even my personal favorite transparency measure, which is reforming laws like the CFAA to allow more scraping, so that researchers like the ad observatory at NYU can do truly independent analysis of what Facebook or YouTube or whoever is showing people. Even reforming scraping laws, that has a privacy issue because scraping is how we got Clearview AI. There is a countervailing interest to think about in that case also.

[00:44:06.92] Last set of countervailing interests is the First Amendment rights of both platforms and speakers. And I think that Eric Goldman will be talking about this later today. So I'm not going to belabor it too much. But there are basically two sets of problems here as I see it. One is something that Eric has written about, which is some transparency mandates make it very, very easy for the enforcer, such as Texas Attorney General Ken Paxton, to come to platforms and effectively strongarm them to change their policies.

[00:44:40.28] And this isn't a regular jawboning question. It's not the way that any state actor can coerce or strong-arm a platform or some other company. It's specific to the fact that the enforcer gets to say whether a disclosure of policy was accurate or not in light of what specific posts the platform actually took down. So it really becomes a question about speech, where the enforcer has power, a power that Ken Paxton has already started using against Twitter in a lawsuit that was pretty expressly retaliatory for them deplatforming Donald Trump.

[00:45:17.79] So there's a state abuse problem here. And then there's a separate, like far less sexy issue that ties to the competition points I was making before, which is if you have smaller platforms having to do elaborate transparency measures, like very, very detailed aggregate transparency reports, it is much easier and cheaper for them if they simplify their speech policies and don't have the more nuanced policies that places like Discord want to be able to have.

[00:45:47.19] And so that becomes sort of state action causing a reduction in the diversity of forums for online discourse and the diversity of speech rules that users can choose. And importantly, this is not just a question about the speech rights of platforms to set their editorial policies, although that's pretty much the only argument being raised in NetChoice. This is also a question about the speech rights of the rest of us as internet users not to have the speech rules we live on under kind of secretly influenced by Ken Paxton or by AJ Bonta in California and any state actors.

[00:46:24.80] OK. So there are all the factors, everyone. How do we balance them? I don't know. I think a really important part of the question is to have researchers or like the people who want to use this data be very serious about what specific data they need for what specific goals, so we can understand where the most important things lie on that side. And then on the other side, like we need more surveillance experts in the transparency conversation. We need more people who can dig deeper into all these countervailing interests.

[00:47:03.89] Ultimately, I think that what we need is carefully designed laws that try to avoid some of these problems, and many of them can be avoided through better drafting. But to make lawmakers have better drafting, we need some kind of standard of review that forces them to do it. And to my mind, that's something like intermediate scrutiny, where there has to be some tailoring of how the law is designed.

[00:47:30.83] But transparency laws are still possible. They're not totally precluded. Unfortunately, what we are seeing in the NetChoice case instead, litigating the First Amendment part of this question, is the platform saying strict scrutiny applies, so you really can't have transparency laws at all. And the state saying, no, this very permissive standard under a case called [INAUDIBLE] applies, and these laws are fine, which they aren't. They definitely could be improved.

[00:47:58.64] And so I'm afraid that we're kind of not in a posture. Well, the 11th and Fifth Circuits have already upheld the laws in Texas and Florida. And so unless this goes to the Supreme Court and they do something smarter, we may not be in a situation where we're going to get the kind of tailoring that I think we deserve with these laws.

[00:48:19.36] DAVID SULLIVAN: So thank you, Daphne, I think, in articulating among many things in that presentation this interplay between whether it is innovation, competition, expression, privacy. You basically touched on the through line of the conversations that have been happening here at Silicon Flatirons for 20 years. And so that's a perfect place to go.

[00:48:45.61] So one thing that occurs to me coming out of that is that multidisciplinary aspect of this and the sort of interplay between say privacy interests and transparency and whatnot and the need for more different types of expertise in the room. I'm curious if Alex or Bri could speak a little bit to what that looks like inside the company in terms of making sure that those kinds of viewpoints are represented when considering why and how to adopt, whether it's transparency measures or other aspects of your work.

[00:49:23.07] BRI RIGGIO: Yeah. So sorry, if I'm understanding the question correctly, it's how does transparency or how do these transparency requirements impacts the actual work behind the scenes essentially?

[00:49:33.57] DAVID SULLIVAN: Yeah. And what does it look like inside a company when you're like, oh, OK, we're thinking about this from sort of as you're developing platform policy, but what about the privacy kind of dynamics?

[00:49:45.63] BRI RIGGIO: Oh, yes. Absolutely. So yes. I would say when my team, when we're drafting a policy, when we're thinking about what are all of the different perspectives, what's more the multi-stakeholder folks that we want to bring into this conversation, we are always thinking about, OK, well, what does this look like publicly? What does this look like if this document were ever to be made public, even if it's intended to be an internal document. Does it does it kind of stand up to that scrutiny?

[00:50:15.42] I think when we think about issues of privacy, in particular, user privacy, that comes into-- so I should back up and actually explain, when we are drafting our platform policies, we think about them as kind of two parts. The first part is, of course, the actual policy. What isn't allowed? What is allowed? What are the criteria that basically our safety teams will be looking for when they're going in to actually determine is this a violation? Is this not a violation?

[00:50:43.80] And then the second part of it is actually the enforcement guidance. If our safety team were to discover this violation or to see a violation, what is kind of the proportionate

response here, and then what do we actually say to users? What is that public facing language that goes out to a user who has committed a violation? What does that look like? How does that interact with the policy?

[00:51:04.29] A lot of the time our policies can sometimes be very academic in nature. And so we always want to make sure that we're translating that policy to users in language that they can understand. And then of course, you think about what about non-English and international language? And you have just a whole enforcement kind of ball of challenges to solve essentially.

[00:51:26.76] When we're thinking about privacy then too and also kind of disclosing the actions that we're taking, I'm trying to think of the best way to get at this question. When we're thinking about disclosing actions that we've taken, we do always consider privacy as part of this. And essentially, OK, if in disclosing that we have taken action here, what happens if the action was happening in a private space?

[00:51:54.99] And Discord, for those of you who are unfamiliar with it, is very much based around private, intimate, invite only spaces. We do have lots of public spaces, but the vast majority of the platform at this point is very private. And so we're always thinking about, from the enforcement perspective when we're drafting these policies, OK, if we disclose that we took an action here and that a policy was violated, is that actually unintentionally violating an expectation of privacy that our users have particularly in these private spaces? And so it's something that we're always thinking about as we're drafting policies but typically from enforcement and then also thinking about what is this going to look like kind of publicly when it comes out?

[00:52:51.33] ALEX WALDEN: I'll just like maybe to linger on that and say, you know, I think it is true that sort of, at least in a large company, we do have sort of the microcosm of all of those stakeholders, from privacy, from freedom of expression, from trust and safety, from legal, from public policy having a conversation about what are the ways we can be more transparent, and what are the challenges around that?

[00:53:14.17] So like the sort of liveliness of the conversation we can have in this room is also mirrored inside the company when we're thinking about what we can do, which is I think also why it sort of takes a long time for us to figure out what is something we can do that is meaningful to the public or other stakeholders that we're interested in providing this for. And also how do we do it in a way that is protective of our users and the policies that we've created?

[00:53:38.68] And then the other thing just to say about that is that's also why it's so important for us to be tailored in the way that we're thinking about how we do transparency across different kinds of products because it looks different for us to be kind of think about what policy transparency looks like on something like search, where we release the entirety of our search rate or guidelines, versus ways in

which we think about metrics that might be useful on platforms like YouTube, where we are creating things like violative view rate and kind of thinking about new metrics that might be useful for people to think about.

[00:54:08.74] So I think that's just kind of a tangent a little bit, but thinking about why it's important to not be too rigid in the way that we think about transparency and kind of being overly prescriptive and standardized in the way we think about it because it should look different across different types of platforms when we're taking into consideration all of these interests.

[00:54:29.40] DAVID SULLIVAN: I think that goes to Daphne's point earlier in terms of if you create transparency requirements that are too sort of blunt, then you lose the benefits of having different types of products. And I think it's one thing I've noticed that I hope to explore as this conference goes on.

[00:54:50.16] My sense, and this is from a distance and maybe ill informed, but folks like Margo and others can correct me if I'm wrong, that in the data protection and privacy space, for example, the benefits as well as the risks of data processing is something that is kind of well factored into these things, whether it's from a company perspective, a regulator perspective.

[00:55:15.03] And that when it comes to content issues sometimes, I think we don't often think about what are the benefits of having this type of content, of having this type of product, as opposed to just we go because there are these very scary risks around things like child safety, terrorism, and violent extremism, et cetera, that sometimes foreclose a more sophisticated discussion about specific products, specific services, and what kind of transparency is useful for them.

[00:55:41.77] So I want to take that moderator's prerogative to ask one more question of the panel before we go to Q&A and bring the audience in. I'm curious. So picking up on something that Alex had mentioned in terms of the change in the conversation, I'm curious whether all of you in the time that you've been working on these issues have seen what kind of shifts in the rationale for transparency being kind of a key aspect of policymaking in this space have happened, and where do you see this going in the next two years, five years, whatever period of time you'd like to forecast?

[00:56:25.76] DAPHNE KELLER: So maybe I think my time range is longer than anyone else, so I'll go first. That means I'm oldest. So I was at Google when they put out the first ever transparency report. In fact, we didn't know that we were coining the word, the phrase, transparency report. I'm blanking on the year, 2013 or something. No, longer. 2010. Yeah.

[00:56:52.66] So the whole point, as we saw it then, was to show how governments were shaping online speech or getting access to

people's private data. It was transparency about state influence on platforms. And there's been a huge shift and an appropriate shift since then to seeing transparency reports as also or maybe primarily disclosure is about platform power and what platforms are doing in relation to speech. So I think that's a really important shift.

[00:57:27.40] BRI RIGGIO: Yeah. I can chime in strictly from just how I've seen things change at Discord as a startup company. I joined the company three years ago. As I mentioned, I originally kind of started on the trust and safety actual enforcement side before I jumped over to the policy side of the house.

[00:57:46.00] And back when I joined Discord, it was pre-COVID pandemic, much smaller company. And there was definitely transparency around communication of policies, but it was not, I would say, kind of at the forefront of a lot of conversations. There was focus on content moderation on making good content moderation decisions justified and reasonable content moderation decisions, but the communication of those decisions was, again, we were doing it, but it was not kind of at the forefront. It was not leading the conversation around content moderation.

[00:58:19.72] Over time, I think as the company has gotten a lot bigger, and then of course thinking as well, knowing the Digital Services Act is kind of on the way, there are these regulations coming down the pipeline, which is a little bit of a forcing function certainly. But the conversation at least with being a part of a startup company that has been maturing over these years, transparency has definitely moved to more of the front of that conversation.

[00:58:46.39] And really kind of scrutiny and wanting to make sure that we are actually being transparent with our users, and we're being clear with them that when we send them language around a violation, it is actually discussing the violation. It's a specific and as nuanced as we can get it. So it's an iterative process. But just in the three years that I've been at a startup company, just for kind of comparison or insight into a platform that is a little bit smaller than some of the other big tech giants out there, the conversations definitely change as the company gets larger.

[00:59:19.72] DAVID SULLIVAN: Evelyn.

[00:59:20.89] EVELYN DOUEK: I mean, I would say, and my time frame is a lot shorter. But I would say I think the conversation has gotten more sophisticated in the time that I've been in this space, I think, due to the product of a lot of people, a lot of people in this room, and outside, a lot of hard work. And so for all of the concerns and things that we have about regulation and things like that, I think that's a million steps ahead of where we were even five years ago.

[00:59:53.60] And so I think that's very encouraging. I think it's also gotten more interdisciplinary, which I think is great to your point,

David. And I think that there's a lot more work to be done in that space. But I think if I can just sort of give lawyers a bit of a knock here, I think lawyers really dominated the conversation for a very long time about what kind of transparency might be good or not, and that resulted in these kind of blunt transparency measures that might look a lot like what we want from transparency in the law, which is like appeal rights, reasons, numbers of individual cases.

[01:00:28.09] And I think there's more awareness now about the systemic kind of transparencies that we might want, as opposed to that kind of individualized transparency, which I think is really important. One of my favorite examples about this is that the oversight board when it first got set up was very much in that individualistic model. But it insisted that it wanted access to the algorithm. And it's like what does that mean, right?

[01:00:54.22] These lawyers, these human rights lawyers, I have a lot of respect for a lot of them. But we need other people in the room saying there is no such thing as the algorithm. And even if you could see the algorithm, like it's not going to tell you what you think you want to know. And so I think having other voices in the room has been good.

[01:01:10.82] I would also say there's been a bit of a turn against transparency in the time that I have been studying it. It was sort of all the rage about five years ago. And it was something that everyone was asking for. And I think now, there's been a lot more sort of-- And I think that might be a product of it being a more sophisticated conversation, more awareness of the costs and more awareness of the trade-offs. It might also be a product of the regulators that we see now who are different to the regulators that we saw five years ago. But it is a noticeable shift in the sentiment around it.

[01:01:47.08] DAVID SULLIVAN: Alex, you basically already answered this question. Is there anything you want to add?

[01:01:51.07] ALEX WALDEN: I mean, because I would plus one everything everybody else said. The only thing I would add is maybe just what I see personally inside my company and in the conversations we're having, is there's a heavy veneer that is compliance-focused. And so I think that over time, it'll be interesting to see what that means for this community of stakeholders who are really focused on what are the creative new things we can do.

[01:02:12.35] And I think as companies are putting more and more effort toward building, like becoming more regulated entities and building compliance mechanisms inside the companies to make sure we're meeting those demands, that we will see sort of what impact that may have on companies' kind of proactive innovation around new and interesting transparency things.

[01:02:36.79] DAPHNE KELLER: Just to kind of merge what Evelyn said and what I said, I think at the same time, partly because of this shift

from people being interested in transparency about government action to platform action or wanting due process or appeals when people are silenced through government action, to wanting similar rates for platform action, we've kind of carried over, as Evelyn said, all these conclusions that we reached back when we were talking about government power and assume that they're the right conclusions for a platform power.

[01:03:09.40] And maybe they are, but the scale is just so phenomenally greater. And they're different in other ways. I feel like if you're in international human rights, this is kind of the transition from the Manila principles, which are all about state-initiated takedowns of platform content, to the Santa Clara principles, which are all about platform-initiated. And I'm not sure if we kind of stop to think through how the details should work.

[01:03:37.13] DAVID SULLIVAN: So it's now time for questions from the audience. Very much in keeping with the Silicon Flatirons tradition and the Phil Weiser Rule, we are going to start with a question from a student. And so I see Blake pointing at someone in particular. I think there should be a microphone coming your way for the online audience.

[01:04:08.31] AUDIENCE: I do have a question for Bri. I was just hoping you could speak more about that education of users that you're doing. I hadn't thought of platforms in the role of educators. And I know that it's a broad scope between innocent actors and really malicious actors. But could you speak to the role of the platform as a compliance educator?

[01:04:35.56] BRI RIGGIO: Yes, absolutely. So again, I'm going to come at this through the lens of platform policy, my area of expertise. When we're thinking about enforcement actions that could be taken against a user for posting something or behaving in a way that is violative, right? There is not with every content area, I think. Again, there are those kind of high harm areas where physical imminent harm is possible. And so maybe not in some of those cases.

[01:05:02.95] But in situations where maybe the violation is less harmful, we can think about enforcement actions besides just kind of the binary like leave up takedown content, leave up take down accounts. And instead, think about things such as like educational warnings. And so when then we would say, OK, I think misinformation is actually a really good example here. And I can think specifically about Discord's health misinformation policy, which we have a blog post about. Encourage you to go read it.

[01:05:34.78] When we would come across or if we were to come across users who are posting misinformation about, say, COVID vaccines, any kind of health misinformation, and there does not seem to be actual context to kind of show, oh, this person is actually deliberately trying to mislead people. Maybe it was just an honest

mistake. They thought that they were sharing information that was helpful, and it actually turns out, ah, that was a misinformed kind of take.

[01:06:00.46] We can think then about sending a warning to that user to basically say, hey, we took down this piece of content, or we took action against your account for these reasons. It was posted something that was kind of misinformed. Here are actually resources to authoritative sources, where you can go and check and see, like, oh, this was why this was misleading or what the actual information is.

[01:06:24.34] And so that's one, I think, area that's a little bit of a low hanging fruit, is to just think about, yeah, when you're taking enforcement actions, where are there opportunities to tell users, hey, actually, this isn't allowed. This isn't something that we want to condone. Here are resources for you. I think about this a lot too in terms of content areas where users might be at risk of committing acts of self-harm, for instance. And that's a little bit I guess away from the education piece, but thinking about where can we help support users.

[01:06:57.88] And then I will also say too with Discord in particular, because of the nature of the way the platform is built, which is really based around communities, any way that we can also empower our moderators. So I'll explain very briefly. Discord is set up around communities. We call them servers. Anyone can go and create a server. And then if you are a server owner, you can basically bring in other users to be moderators or administrators, and they can help set the rules and norms of the server. Everyone has to abide by the guidelines. You can set rules above and beyond that. It's a community-based kind of approach.

[01:07:32.54] There's also opportunities to kind of teach community leaders, hey, here's how to also kind of educate when you see potentially problematic behavior happening. And so for instance, we have a Discord Mod Academy. We have a whole kind of curriculum of what it's like to be an effective online community moderator that we make available. And we have a program. And so that's another area where we can try and be a little bit more educational and supportive, versus just strictly punitive.

[01:08:00.12] DAVID SULLIVAN: So other questions? Let's go first to the rear, and then come forward. And I should have said, actually, if folks could be sure to just identify themselves when asking a question. Thank you.

[01:08:17.59] AUDIENCE: Hi. Thank you all for your time. My name is Gabe Burdon. I'm a 3L here at Colorado. And I was wondering if you could discuss your opinions about like the almost de facto deputation by public sector authorities for private sector companies and for discussing what they consider to be disinformation or malinformation or misinformation, and maybe transparency with respect to, I don't know, more of a public discussion about the extent and of that

relationship and levels of comfort that high level executives in certain large companies think they should have with our government, and where that line should be drawn, and the public has a right to know more about it.

[01:09:10.22] DAVID SULLIVAN: So I do want to just take the other question first because I feel like we could spend the rest of the time responding to that, which is really great. But I think there was one person just, yeah. And then we can bundle these and respond.

[01:09:24.22] AUDIENCE: Hi. My name is Yamiche. I'm from the School of Business here. My question is, let's say if we are a policy maker dealing with transparency. Do we, in 2022, have all the tools and technology to actually implement what we want to, or if there are any gaps, is there enough research in the area?

[01:09:50.15] DAVID SULLIVAN: Great. So both questions, who wants to jump in first?

[01:10:00.59] DAPHNE KELLER: OK, OK. So the first question I could definitely talk about for several hours. But there's this foundational issue, which is that lawmakers or people who are state authorities have very limited power under the First Amendment to prohibit disinformation. There's some disinformation out there that's so bad, it can be illegal, consistent with the First Amendment. And then there's a really broad swath of disinformation that people are worried about that's probably lawful.

[01:10:36.02] And so it's not even that they're delegating a power they have to platforms. It's that they want platforms to go out and deal with that stuff. And only platforms can do it because the platforms are not constrained by the First Amendment, which is in many ways a very problematic dynamic. It means that we are necessarily handing policing power to these big private companies, over which we have very little oversight, and very little control, and so forth.

[01:11:07.67] But if you're not going to do that, what are you going to do? Do you have a conversation about shifting the First Amendment line and making there be more content that government can legitimately regulate, like where does that go? So I'll pause there. And then I do want to speak to the second question about whether we have the technology to measure the things that we want.

[01:11:26.81] And I think there's a really important kind of measure being discussed right now, where I'm not sure we really do generally have the technology. And that is measuring the so-called prevalence of particular content across a platform. So this is instead of saying, well, we know what we took down and why, so we're going to be transparent about that number. It's asking about all the content that hasn't been reviewed and trying to estimate across all of that content how much of it violates the hate speech policy and so forth.

[01:11:58.54] And both Facebook and YouTube have come up with ways that they try to extrapolate those numbers. And at least Facebook, and I hope not YouTube, is in DC and state capitals telling lawmakers they should mandate everyone to do that. And I think we need to ask a lot of questions, in particular, about how well this works for languages other than English, or for people using slang that is different in Peru versus Spain. I think there's a lot we should be asking about the prevalence metric.

[01:12:32.81] EVELYN DOUEK: Yeah. So I want to plus one everything Daphne said and read it into my remarks and just echo particularly the point about the constraints on the government action is what makes content moderation so useful and important. Like I am deeply suspicious of private power and concerned about the level of power that these private companies have over these fundamental self-governance interests. But it also can be really important because in some ways, giving that power to the government would be worse to allow the government to police many, many different kinds of false information.

[01:13:11.22] But I do think there is this content moderation hot potato thing that happens a little bit because these decisions are also really unpopular and controversial in many cases. And so you see people, like institutions trying to throw the potato to each other. And we saw in the pandemic, for example, which was the first time that many platforms came out and said, we're going to take content down purely because it's false, purely because it is misinformation or disinformation.

[01:13:38.55] And it was kind of like this big moment for watchers in this space because they had so long insisted, we're not going to be arbiters of truth. But the reason why they did that, the way in which they did that, most of them said, well, the reason why we can do this here is because there are accepted authoritative sources that we can point to to make our policies in terms of disinformation, and that was normally like local health authorities, places like the CDC, places like the WHO.

[01:14:08.30] And of course, as the pandemic went on and there was sort of more information about how sometimes those authorities had got it wrong, there was finger pointing. And it didn't have quite the legitimizing effect, I think, that the platforms want. I also think that there are legitimate questions to be asked about government and platform relations in this area as well.

[01:14:32.52] And this is one of the reasons why we want more transparency from governments, as well as more transparency from platforms because one of the concerns we would have is that governments do an end run around the First Amendment by not making laws explicitly saying we outlaw certain kinds of mis and disinformation. But by quietly jawboning came up earlier about putting pressure on or behind the scenes, suggesting the platform should take down certain kinds of information. So you know, I'm not a conspiracy

theorist in this area. But I do think that there are justified questions about the nature of those relationships.

[01:15:10.68] I think the second question is a really, really important one. And I think the answer is, no, we don't have the tools. And that's why I have deep concerns about enshrining into law transparency measures that are really easy to draft, like that are just like give us the number of things you take down, but not so useful. And wanting to have a more flexible regime, I guess, transparency regime that can adjust over time as tools get better, rather than for exactly the reasons that Daphne said, that the big platforms are in favor of these transparency measures is often because you can become a tick the box compliance regime that doesn't really get to the useful information.

[01:15:56.82] DAVID SULLIVAN: So I think that brings us to the end of our time, but also perfectly tees up-- oh, we do. Oh. Oh, wow. All right. Well, I want to add one thought of mine, and then we can go back to the audience here. But on the question of tools, I think one thing that I've been thinking about lately and that may be an under-explored aspect of some of these discussions is that we tend to focus on companies like Google and Discord, the providers of services.

[01:16:28.67] And there are a lot of companies out there who are providing services to those companies when it comes to identifying hate speech. ML classifiers, that sort of thing. And those vendors and sort of what kinds of tools they're bringing and what effectiveness of those things, I think, is an underexplored area that I would recommend to folks who are looking into this area because a lot of those companies are really in growth mode right now. And especially at very small companies, they may be doing everything. So yeah.

[01:17:06.53] DAPHNE KELLER: Search the vendors. I think that's the translation, right?

[01:17:11.09] DAVID SULLIVAN: Yeah. Yeah. So other questions from the audience over here? Yeah.

[01:17:22.42] AUDIENCE: I would venture that most of the people in this room went to law school because they were like me, and they couldn't do math. And Evelyn talked about the algorithm, and that's really curious to me. And I think your point was that everybody seems to want the algorithm, but it's not really going to give them the information that they want, or it's not the cure all that they think it's going to be. And I was wondering if you could expand on that a little bit, as to why the algorithm is not going to be the holy grail.

[01:17:53.89] EVELYN DOUEK: I think probably the practitioners are going to have more useful information about that. So I think, first of all, there is no such thing as the algorithm that gets used at these companies. There's multiple different kinds of tools that do multiple different kinds of things. And so the tools, the automated technology

that platforms use to take down hate speech is different to the tools that they use to take down.

[01:18:21.76] Terrorist videos is different to the tools that they use to amplify or deamplify content in their feeds. And it's constantly changing, all of those tools are constantly changing. Another reason why it would be very limited is because first of all, if you could see what the factors are that feed into those tools, that's not so useful or interesting without knowing what the data is it's being fed into that. So you could have sort of information.

[01:18:52.27] And you know, honestly, there is information, like Facebook has released quite a detailed description of the factors that go into how it prioritizes information in your feed and how many different variables go into that. But without knowing sort of what it's being trained on or what it's looking at, it doesn't tell you very much about what's actually happening on the platform.

[01:19:15.79] AUDIENCE: So the GOP has sued, I think, it's Google, over their algorithm, saying that basically, if it says GOP, conservative, everything's getting blocked, or it's getting sent into a spam filter, or it's being sent off, so that the end user doesn't get it. So I mean does the algorithm look for just-- is it more complicated than just one word, like liberal, or conservative, or GOP, or Ted Cruz, or whatever it is that's in the email?

[01:19:49.69] ALEX WALDEN: Yeah. Just sort of repeat everything that everyone said. But there are many algorithms, and they are being regularly updated all the time. Like still my favorite stat is that 15% of searches are new every day. And so that just kind of goes to show the ways in which the algorithms that are in action are kind of being put up against novel questions and new sets of information on a regular basis. And so then we are adapting, and amending, and revising those things all the time, one.

[01:20:19.18] Two, all of the research that has been done thus far demonstrates that those sorts of assertions don't have a basis. That is not actually happening. And so I think that's maybe speaks to the importance of having research done on the platforms to really be clear about what is a myth about what's happening and then what is actually happening. What are the outcomes of what our recommendation algorithms and other things are doing.

[01:20:46.67] And then last, just to highlight, I think YouTube does have a paper kind of explaining how its recommendation algorithm works. And I think that it gets to especially those things that are factors about what's considered to help folks understand more generally what's happening without a specific interrogation of the ones and zeros.

[01:21:09.63] And then lastly, I think there's other things that have been interesting in this space to look at. Like not really in the content

moderation space, per se, but in other product areas we have. Like in Cloud, we do model cards where we sort of talk about what we've built, and the accuracy rates, and what it can be used for. And so it's other ways of thinking about how you can look at the performance of AI and ML, what it's doing measured, against what it's supposed to be used for. So just another thing to throw out.

[01:21:37.86] DAVID SULLIVAN: I'm wondering whether maybe just, Daphne, as somebody who's written extensively on amplification as a concern, an anxiety of the public and policymakers and the challenges about what does that mean. If you could speak a little bit to recommendation and amplification, and why that is maybe not as easy or as simple a thing to regulate or approach with law and policy as folks might think.

[01:22:07.08] DAPHNE KELLER: Sure. And this dovetails really well with the last question about algorithmic transparency. So for anybody who is interested in this topic, I really recommend the work of Jonathan Stray at Berkeley. He's been publishing things with coauthors on this recently, going into questions of what would be useful to know about algorithms? What does good transparency look like?

[01:22:28.38] And also publishing things that relate to this question, which is what would it mean to regulate amplification or say that platforms are liable for increasing the reach of particular content? So my article, Amplifications and its Discontents, looks at this as a First Amendment question. And Jonathan's comes at it very much as like a statistical question or a computer science question. Like literally, what does this mean?

[01:22:56.97] And one thing that his students or his research group did was go and ask policymakers, what do you mean by amplification? And they came up with three very different answers. I can't remember all of them. But one of them, which I think is very common, boiled down to showing one thing instead of another thing. When there are infinite things, or trillions of things, or even just millions of things that could be shown, which ones are you showing? Well, that is the basic act that any platform is doing in the UI that you look at any time. And so that can't be what amplification means.

[01:23:35.20] And I think that for some platforms, like Twitter, you can imagine just a reverse chron order feed as the non-amplified baseline that you then compare against to say whether the ranked feed caused greater distribution for harmful or illegal content. For other platforms, like, well, Google web search, if it doesn't rank things, it is useless, right? Like nobody wants a version of web search or any kind of search functionality without amplification.

[01:24:10.42] And then for a product like YouTube, setting aside the recommendations part, like when you go to YouTube, what do you see on the page? Are they supposed to have it in reverse chronological order, so that any time you show up, you just see whatever was

uploaded most recently? So there are a lot of problems in defining what we think the relevant baseline is, both for kind of statistical reasons that Jonathan goes into, and then for these practical reasons about what is it we expect from these products.

[01:24:42.28] DAVID SULLIVAN: So I think we have time for a couple more questions. So let's go first here. Yeah. There will be a mic coming to you. And then we'll go to Jeff.

[01:24:52.08] AUDIENCE: Thank you. Fascinating discussion. And in particular, it was interesting to understand how we look at the changes that have been happening in the platforms over the recent years. As someone who has lived in the bits and bytes, when these platforms were kind of growing, I very vividly remember that the tone was, or actually, the responsibility was given to the product managers, to the engineering managers to make real important decisions on these platforms.

[01:25:23.67] It was innovation comes first. And what does it go, fast break things. Just do things. And I remember being a product manager myself, I had to make the choice of do I do a default opt in or out, and am I taking the data? Am I not taking the data? And these companies played the role of hands off, right? Like we're just a platform. Someone else should regulate what's happening here.

[01:25:50.19] We're fast forwarding 10, 15 years into where we are today. And my curiosity is, A, are we seeing a trend similar to what we saw in the EU, for example, not on transparency, but on privacy with GDPR, just blanket statements of the right to be forgotten, I own my own data, and things like that. Are we going to see that in the US?

[01:26:11.37] And secondly, it feels-- I remember Facebook did a very courageous move and said no one's going to be anonymous on the internet. Whereas I go now into Discord, which my kids are on, which there is no one who's not anonymous, right? There's encouragement to not-- like none of my kids have their name on there.

[01:26:33.18] So from a transparency perspective, it feels like the trend is going the other direction. And there's this space for the regulators to come in and do these blanket statements. And do you foresee them coming in at that level, kind of what the EU did on data, but on transparency?

[01:26:52.14] DAVID SULLIVAN: So I think in the interest of time, maybe we have that as the last question and allow our speakers to offer any final thoughts in response to that. So I don't know if we want to start here with Discord.

[01:27:03.53] BRI RIGGIO: Yeah. I mean, in terms of-- I don't know that I could speak to what's coming from a regulatory standpoint. I would much rather leave that kind of question to potentially my public policy

friends or legal friends who are kind of more attentive to that landscape.

[01:27:24.11] What I can say, though, is I mean, to the idea that product managers or engineers were potentially one day, long ago, making a lot of those decisions. I mean, I think that that's true in a lot of startup environments as well, where maybe policy is really kind of not at the forefront of those conversations when you're first trying to kind of stand something up.

[01:27:45.62] At Discord, for instance, I mean, I run our platform policy team, but I also have a counterpart who really focuses on product policy now. And there is kind of this responsibility that I think we've taken on as a company. I mean, we also have someone working on responsible innovation, trying to look at what are the externalities to society of some of these product decisions that we are making around - yeah, any time we're developing a new product, what are the implications there for reach of content? What are the implications there for privacy?

[01:28:13.82] And so my product policy counterparts and the team there will work with those engineers and product managers to really try and think about, OK, what's actually happening here? And there's also now the addition, of course of our legal team, thinking about, OK, given the regulatory landscape, how do all of these different things kind of play together?

[01:28:35.39] And there's potentially sometimes some tension there between, OK, are we doing things safely? Are we doing things kind of in a deliberate way that we want these products to be developed, that's going to actually kind of safeguard users, safeguard the platform, take into consideration privacy?

[01:28:53.93] And so again, I can just again speak to my observations over my time at Discord, which has been there is a sense of responsibility that I think has been taken on there. That it is the responsibility of the platforms. Whether or not the regulations are coming, that just happens to be one factor.

[01:29:12.80] DAVID SULLIVAN: Any final two-second thoughts from the rest of the panel? OK, well, I think that's a great place to wrap here. So thank you to our panel. Thank you to the audience for all the great questions. And looking forward. I think we did a pretty good job on why transparency.

Keynote: Julia Angwin

<https://www.youtube.com/watch?v=xJDPBn2OZFA>

[00:00:01.07] SPEAKER: --body a couple of moments to trickle back in from coffee, during which time I would like to introduce our first keynote for the day. I'm delighted that we can be joined here by Julia

Angwin. Julia founded the markup to produce [INAUDIBLE] data-centered journalism about technology, and the people affected by it.

[00:00:24.09] So her voice today is in some ways the missing link between platform transparency, technological transparency, other individualized forms of transparency, and potential catalysis for policy change. Before founding The Markup, Julia Angwin led investigative teams at ProPublica and the Wall Street Journal. Author of the book *Dragnet Nation, A Quest for Privacy, Security and Freedom in The World of Relentless Surveillance*, and *Stealing MySpace, The Battle to Control the Most Popular Website in America*.

[00:01:01.25] She has a BA in mathematics from the University of Chicago, and an MBA from Columbia University. Julia Angwin is a winner and two-time finalist for the Pulitzer Prize in journalism. So the way that we'll format this today is that we'll hear from Julia first for roughly 30 to 40 minutes, after which I'll ask a few introductory questions, and then we will turn it over to you, the audience. So please keep your questions in mind. Thank you.

[00:01:33.49] JULIA ANGWIN: Hello, it's great to be here. I'm hoping you can all hear me, and I'm really sorry that I couldn't be there in person. I really wanted to be. I've been many times to Silicon Flatirons and loved it and love the conference. It feels like today is a great day to be talking about tech and transparency. If there is any lesson from this week on Twitter, it feels like the one thing maybe we could all agree on is that having one billionaire make all decisions about speech governance and public discourse is maybe not the optimal choice.

[00:02:16.94] So I think there are a lot of ways to solve this, like Margot was saying, and you guys, I'm sure, are talking all about policy and technological issues. I want to talk about the role of journalism and the journalists and how we try to hold tech accountable for the decisions that they make that are often hidden behind an algorithm.

[00:02:40.83] And so I have been writing about privacy, algorithmic bias, et cetera, for more than a decade and leading teams of engineers who have done algorithmic audits. And I wanted to put together a little talk about what does it take to do that type of accountability work because I think we need much more of it. So I'm going to try to share my screen.

[00:03:11.11] I want to talk about what it would take to do-- what it does take to do better journalism in the algorithmic age. Because I think we're going to need a lot more of it. So, basically, I'll just tell you a little bit about myself. I grew up in Silicon Valley. I started programming in fifth grade. I was part of an early generation that use Apple II and really just loved the comp-- it was called the personal computer revolution at that time, and I really thought that I would actually go into the tech industry, but I fell in love with my college newspaper and decided to try journalism for a little while.

[00:03:48.69] So I ended up at the Wall Street Journal for 14 years, ProPublica for four years, and then founding The Markup four years ago. And I have started to think of what I do as mathematical journalism, which sounds kind of pretentious, but I think what I mean by it is using the power of math to break important stories. It's, I think, an underused piece by journalists, many of whom went into the field because they hated math.

[00:04:19.68] So I want to just describe a few things I mean by that. So one story that I think some of you might be familiar with was something I did at ProPublica about criminal risk score algorithms and whether they were biased. And this was a question that legal scholars, including many at Silicon Flatirons, have been raising forever that the idea of coming up with a predictive score about whether someone would commit a future crime was legally questionable and very likely to be bias based on the kinds of questions that they asked.

[00:04:54.45] But it wasn't until we collected the data and ran the numbers that we were able to show that it was actually bias. So I collected 18,000 different scores. We showed that even just looking at the scores of whether a white or a Black defendant was given a high risk or low risk score-- you can see the difference here-- the white defendants were given a preponderance of low-risk scores.

[00:05:21.03] And Black defendant scores were pretty evenly distributed 1 through 10, high risk to low risk. And so the question that raised was, are the white defendants really all just Mother Teresa, or was there something else going on here? So what we needed to do was check to see whether those scores were actually correct.

[00:05:38.38] So we went on to check and see whether the people who had been predicted to commit a future crime in the next two years went on to commit that crime. And what we saw was it wasn't that accurate. The score itself was actually only 60% accurate, but it was biased in the way that was inaccurate. So when it was wrong, it was twice as likely to label a Black defendant high risk when they weren't, and twice as likely to label a white defendant as low risk when they weren't.

[00:06:10.75] And so, basically, the false positives and the false negative rates were skewed, and that kind of error is something that had not been seen before we did this type of journalism. And it did lead to a lot of soul searching in the computer science community, slightly less soul searching, unfortunately, in the criminal justice community, which still uses this score and many others like it but has led to things like Prop 25 in California not being accepted, which was the idea that they would replace bail with these risk scores. Because, people argued, that you shouldn't replace bail, which is obviously a terrible system, but with a system that is known to be racist.

[00:06:55.08] Another story that I think used math to great advantage was a story that we did at The Markup about Amazon, and the question

of whether they were preferencing their own brands. So basically, a lot of Amazon sellers had said, anecdotally, look, I can't get to the top of the search results. If you search for batteries or staples on Amazon, we can't get to the top of those.

[00:07:19.86] We are all down at the bottom, and that means we can't sell. And so once again, we needed to do math to really prove whether this anecdotally was true. So we collected thousands of search results and then ran a random forest decision tree to see whether being an Amazon brand was predictive of being in the top, and it was the most predictive factor.

[00:07:46.08] Being an Amazon brand was the most likely factor to get you to the top of search results much higher than the things you might expect, like star ratings and the number of reviews. And so once again, this was a mathematical way to show something that people had vaguely felt to be true, and it was interesting to me because I was not sure that lawmakers, policymakers would be able to deal with a probabilistic finding like this.

[00:08:11.85] But in fact, it did lead to the house antitrust committee basically saying that Amazon had lied to them when it testified that it wasn't preferencing its own brands and has asked the DOJ to investigate them for perjury. And then finally, there's another story I would just quickly mention about how math can really help unlock something.

[00:08:34.41] So Allstate is a car insurance company, and they had been saying, and still do say, that they have a special secret sauce algorithm that allows them to determine whether you're a loyal customer or not. And essentially, if you're a loyal customer-- this is the cool part-- they'll charge you more. So you get a penalty for being loyal because they [INAUDIBLE] you aren't really going to shop around.

[00:09:03.35] And so they had this, what they called a retention model, and they were filing information about it with different state insurance regulators. And we wanted to see what was happening with this algorithm. What did that loyalty look like? So once again, we ended up using a decision tree to figure out what did the data show, and what it showed was they had a price of loyalty, which was essentially \$1,900 premium or more meant that you were price indifferent.

[00:09:36.85] So they were going to just give you a huge increase each year. And if you paid less than that, then they would decide that you were more price sensitive. You might shop around, and so they weren't going to try to give you a huge increase in price. So this was actually something that hadn't been uncovered by the regulators who hadn't done this kind of analysis and hadn't been known to the public.

[00:10:04.40] And so, basically, they've gotten in some trouble in Texas and in California suing them over this-- we call it a suckers list because the idea was that you're a sucker who they think they can just milk you

for lots of money. And these are the kinds of stories you just really can't do without some mathematical literacy, and I think these are the stories of our algorithmic age. Because, I mean, I guess it's nice that Elon Musk is just declaring what he's going to do, and there's not an algorithmic secrecy there.

[00:10:33.70] But, generally, a lot of companies hide their policy choices inside of technological systems, and so you do have to work to uncover them. And so I thought that I would just spend some time here talking about the lessons that I learned from doing these types of reporting. What does it take to audit an algorithm? So the first and most important lesson is actually, before you even start looking at an algorithm or trying to analyze it, which is to decide what to look at.

[00:11:07.21] I think anyone who follows journalism knows that the choice of what story to write is actually as important, maybe, or more, than the story itself. Because there's a million topics to cover. And if you only write about Donald Trump's tweets, then you really aren't writing about any of the other important issues in the world. And so I think that, oftentimes, most journalism love secret new things, which is, of course, exciting.

[00:11:33.74] But I think the kinds of things that can be really important or really can often be hidden in plain sight. Allstate, for instance, had been saying that they had this model. Amazon sellers have been complaining for years about the way that they were treated in search, and lawyers had been complaining for years about these criminal risks for algorithms. And all of those stories were out there.

[00:11:57.94] They were somewhat known, but what I think is important is that bringing math and data to the table made it much more salient to policymakers and made it something that they can have an argument about. And it wasn't just anecdotal evidence. I think another thing that's really important about data is that it's very tempting to just grab a data set, look at it, and start looking for a story.

[00:12:19.51] But actually, that is the road to ruin. I know because I've done that many times, and the reality is that if you don't have a hypothesis first, you're not going to get a good story. And so the hypothesis has to be something like, I've heard from lots of sellers that they're getting disadvantaged in search. What data what I need to support that, and then what can I do to build a testable hypothesis?

[00:12:45.23] And that is just like all reporting, starts with a tip or a hunch or some sort of information. I think data reporting, sometimes, people get confused about whether it needs to start that way, and it absolutely does. It's also important to remember that data is political. Whoever collects it, gets to organize it. And we've certainly learned that with Facebook. When they have previously released data sets to academics, people have said, look, this data isn't useful.

[00:13:13.85] It doesn't tell us the things that we need to know about what's happening on the platform. And that's true in all regards. There's a reason that there's no national database of police violence towards citizens because there's no political will to collect that information. And so that's why the Washington Post had to build their own database to capture that information, and they won a Pulitzer for it, as they should have.

[00:13:39.62] And so I think it's also really important to remember that we always, as journalists, would love to get a nice data set from a think tank, but that is already going to be curated to give us the answers that they want us to have. And so we often have to collect our own data, which is why I built a newsroom with engineers in it who could scrape large data sets for me.

[00:14:02.33] It's also important to remember that journalism has a trust problem, and we need to overcome that. The idea that you could just interview three people in a diner and say, this election is all about whatever that those people told you. I mean, people still do those stories. But I think the public is really over it. They don't believe that anymore. That's one of the reasons for skepticism about journalism, and so I think it's important to think as journalists, what is the right sample size that would allow me to declare some kind of finding?

[00:14:35.89] And, of course, like with something like Amazon, we scraped Tens of thousands of search results, but it's a gigantic platform. And so there's no way for us to really know if that was the most representative sample. We did the best that we could, but it was a big enough sample that it meant that this wasn't just a half-assed trend. And so I think that it's important to do the most that you possibly can but also recognize that, as journalists, we're never going to have the perfect sample size.

[00:15:10.28] I think one thing that is challenging about this type of work is the fact that it has to do with statistics, and statistics, it's often just hard to understand. Particularly, things like odds. The odds of this happening are eight to one versus seven to one, which is sort of what the findings were for our Amazon investigation. And yet, I think that getting comfortable with risk, and the calculations of risk, is what we need in this algorithmic world.

[00:15:40.52] Because the systems that we're analyzing are risk measurement systems. Essentially, that's what they are built to do is to calculate risk and look at it and spit out some sort of number. And so in order to analyze those systems, we also need to reverse engineer those risk calculations. And so it's a challenge as a journalist to write things that are statistically literate, but they are I think something that we have to get more comfortable with in our journalism.

[00:16:12.04] That said, I do think that readers just don't want to read a bunch of numbers, except for some, and those people I love, and God bless them. But we do always need a story, and so one of the sad

things about a lot of the investigations that I lead is that we might do six to nine months of analysis, data collection and analysis, to get to a finding, and then we're not done.

[00:16:37.40] We're like, oh my gosh, now we can find the story, and that's where I spent a month knocking on doors in Fort Lauderdale, Florida, to find people, for instance, who had been scored by that criminal risk score algorithm and knocking on their door saying, do you remember being arrested? Do you remember them asking questions? Did you know you've got a high-risk score? And of course, they were like, I don't know. I don't remember.

[00:17:00.19] But without those stories of the two people who are arrested for the same exact crime, and one had a huge track record. He had been arrested multiple times for theft, and he got a low-risk score as a white man, and there was a young Black girl who had no felonies and just a juvenile misdemeanor on her record who got an extremely high-risk score.

[00:17:27.43] And without that sort of story, the findings about the false positive rates and the false negative rates is just not as compelling. And so the challenge for journalists is always to find a way to tell that story. I also think it's really important to know that journalists, we are not experts. I've been covering technology for-- I don't know-- 25 years, maybe more, and yet, I'm not an expert.

[00:17:59.92] I know who to call to ask questions, and I think we have to be humble about our own role because, particularly when it comes to statistical analysis. I have a math degree, but that doesn't mean I'm a statistician. And so we actually set up a process that I liken to peer review, where we actually get experts to review our work and our methodologies before we publish them.

[00:18:24.59] And so, usually, we'll get at least one statistician and then definitely need people who are experts in the area. So criminal data is really different than Amazon data. And so for the story on Amazon, we'd have people who had were sellers, and people who were experts in Amazon search. And then they would advise us on whether we had missed something in the way we're looking at the data. And so that process is sort of like an academic peer review.

[00:18:56.77] And then after we get all those reviews, we actually then go and do what I call adversarial review, which is bring the analysis to the company or the entity that we're writing about and give them all the data and our methodology and say, look, here's what we did. Please tell us where we're wrong because the reality is we want to know where we're wrong.

[00:19:18.67] We want to know if we made a mistake. And so, sometimes, we find really important things that we got wrong in that moment, and that is really helpful because that adversary has the most

incentive to tell us that we're wrong. They want to find a hole in our analysis, and as of yet, no one has found a hole that collapsed.

[00:19:41.43] The analysis, in fact, most every time, it's been something small that allowed me to just tweak and make it more accurate, but the findings always stood up. But if they came back and were convincing about why it was wrong, we would have to abandon the story and that would still be a good outcome because we're in the truth business. I think one thing that is really great about doing this type of data-driven journalism is the fact that we don't have to worry about this idea of objectivity.

[00:20:09.15] I grew up in a world of journalism that taught me that objectivity was the goal, and what that often meant was you got to have people on both sides. And you call somebody on this side and that side of the story. And over time, essentially, that got gamed. So climate change is a perfect example of that, where I think 99.95% of the scientific literature supports the idea that the Earth is warming. And really, the only questions are how fast and by what cause?

[00:20:40.17] And so the idea presenting that as both sides is actually a false equivalence, and yet for a long time, that is what journalists were doing. And I think that, luckily, we have awoken as a profession and stopped doing as much of that. But I think that an even better next step is to find a way to talk about limitations. So what we do in our methodologies when I do these big investigations is we would write about what we found.

[00:21:08.97] Amazon, we found this much of them. They're preferencing their own brands, et cetera. But we do the limitations, which is the limitations of our findings, or we don't know if this is actually a representative sample. We did the best we could. We don't know all the factors they're using in their search criteria. We only tested the ones that we could see. There's always things that you don't know.

[00:21:29.86] And I think that being really clear about that is actually just a really good way to build trust with the reader, which is like, here's what we know. Here's what we don't know. Journalism is not the final take. We're the first draft of history. So it's OK for us to just say, this is what's known right now, and we'll update you when we find more. I think it's also really important to show all of the work.

[00:21:53.01] So we have a habit of publishing methodologies, full data sets, often the code that we use to do our analysis. Anything that we can provide, I think, is really helpful for people who want to work with that data. There are people who find things in the data sets we've collected that we didn't find, and so we're contributing that to the public and allowing other people to do additional research.

[00:22:21.60] And also, it is helpful because people will replicate our research. After the criminal risk score algorithm story ran, the company pushed back on it pretty hard. But many different academics reran the

data, found the same things, and validated our work. And so it ends up being helpful, I think, to journalists as well. And then, finally, I would say the thing that journalists could do better, and that I try to do, is to keep going.

[00:22:53.49] It's easy to just do one story and then never cover a topic again. But the reality is that change in the world comes from constant, repetitive hitting on important topics. Think of gay marriage. That campaign went on for decades before the law was changed. And I think that's how change happens is that a lot of dedicated people keep yelling about something-- or not yelling-- putting important points and data across the table saying why this thing would be a better thing for the world.

[00:23:30.31] And the thing that is really great about building a newsroom that is staffed with engineers and data scientists is that we can sometimes build tools to do automatic, persistent monitoring. So one thing that we built at Markup was something called Blacklight, which is just a tool that we built for ourselves actually to try to analyze websites and see what creepy privacy techniques they were using.

[00:23:54.96] But then we realized we could open it up to the public, and let anyone check any website for creepy behavior, and you can check it out markup.org/blacklight. But since then, many different organizations have written reports like Human Rights Watch and others based on information that they collected on Blacklight. And so that is a way for us to continue to be watchdogs but without having to actually read a story ourselves each time. So that is all I have from my presentation. I'm excited to talk to you guys that have questions.

[00:24:33.95] SPEAKER: So I had a number of different questions. I think your voice is so key to this conversation today, as I mentioned, in part, because journalism is often the catalyst for policy change. And I know you mentioned the ProPublica story about recidivism, risk algorithms, and the Amazon story, and the House investigations. But I wanted to first ask, what are other big or biggest policy changes that you have seen occur as a result of your coverage of the tech sector?

[00:25:10.18] JULIA ANGWIN: Well, maybe one of the bigger ones is the work that I did for many years about Facebook's discriminatory ad targeting platform. So basically, in 2016, I noticed that Facebook had this ability to have a dropdown menu where you could target your ad. And you could just say, I want to target to Blacks, but then you can also say-- it had a dropdown menu to block your ads from being seen.

[00:25:48.18] And so you could block your apps from being seen by different racial categories. And so then I thought, well, could you do that for housing ads because there's a law-- the Fair Housing Act-- that says you can't actually discriminate by race or all sorts of other characteristics in housing ads, and I was able to buy an ad. And that was really shocking.

[00:26:10.98] So I wrote a story saying, I can't believe this. Then Facebook said they would invent a big algorithm to solve this problem, and I remember saying to them, I don't know. Why don't you just get rid of the dropdown that says block Black people, and they were like, no, no, no. That's not going to stop it. We're going to build a big, old algorithm machine learning. It'll be really amazing.

[00:26:30.38] They launched it a couple of months later, and then a few months after that, I was able to buy an ad again and get through their fancy algorithm. By that point, I think HUD had started to sue them, and they said, OK, now, we're really going to work on it and make a better algorithm. And then they got sued by a group of housing groups and did a big settlement and said, OK, we're really, really going to block them now. Because we have even a better algorithm, and then stuff just kept slipping through.

[00:27:02.12] And, eventually, I think, after four years, maybe five, they eventually got rid of the dropdown menu. So you can no longer use race characteristics in housing ads. And I mean, I have to say this is like a really sad story that I'm telling you, like this is some great win. Because this is truly just basic compliance with an existing law. But that's what it takes to bring change sadly in today's world.

[00:27:28.97] SPEAKER: Yeah, so all of these stories that you've mentioned where you've gotten some purchase from policymakers or responses from companies, what was the magic of the moment? What, in your view, made it more likely that there would be a public response or a policy response to a story in hindsight that you thought would be really important? And I guess, conversely, have there been stories where you put something together, and you expected a policy response and public outrage, and then it dropped out there, and nothing ended up happening?

[00:28:03.58] JULIA ANGWIN: Well, sadly, the latter is often the case. This is the thing that is really hard about being a journalist is you have to just believe that change will come, and it might take a really long time, and it often does not come the day you publish. The times that it does happen are times that it's just totally egregious. The time that I wrote a story about how you could buy an ad targeted to the term Jew hater on Facebook.

[00:28:37.12] It prepopulated. So if you were writing into the targeting category, Jew would suggest hater. So they turned that off that afternoon because that was just ridiculous. It went completely viral, and people started trying all different Muslim hater, et cetera, et cetera. And so they had to turn off this whole thing that they had basically created a system that would just no human ever looked at the ad categories.

[00:29:05.46] It just auto generated from things people wrote in their profiles. So if enough people wrote in their profile that they were Jew hater, it would be like, that must be an ad category. So sometimes,

when things are really egregious, you can get an immediate response. To be completely candid, if you are in a brand-name newspaper, the New York Times, Washington Post, Wall Street Journal, you're more likely to get a response. I did spend much of my career in those places.

[00:29:31.86] But these days, even at a small place like The Markup, we can also get responses. And I think data is a big piece of it. This is why I'm such a believer in data journalism. I think that giving the evidence and then allowing other people to work with it, by putting the data set out there, it actually provides the policymakers something to do other than just say, I read a story, and it said this.

[00:29:59.31] I think when the, I read a story that said this works better when it's in the New York Times. So if it's Maggie Haberman, and she's like inside the room, and Donald Trump said this, people are like, OK, that probably happened because she's been right. But if you're talking about something algorithmic that's black box and confusing, you have to show your work. And so that's why, I think, that it's really important to put data out there because I think it allows for policy conversations to take place.

[00:30:29.57] I actually think, despite the major dysfunction we have in our policy worlds, I do think we are somewhat data driven. Both sides do usually have to come up with some sort of data paper about why their thing is better or not. And so if in an evidence-driven world, the more evidence we can provide as journalists, I think the more we can inform a better public debate.

[00:30:52.31] SPEAKER: I don't want to get depressing and say this all assumes that policy making is actually evidence driven, but I just did. But I think I want to revisit the second half of that question. Do you have examples of stories where you did put out something you thought would get policy purchase, and it landed invisibly?

[00:31:15.50] JULIA ANGWIN: I mean, unfortunately, that's so common that I'm actually having a hard time coming up with an example, but let me think about it. There have been some stories like that. So here's a good one. So Amazon, we did a big investigation about how they had a list of products that they said they weren't going to sell that were deadly, essentially. Things that would kill people.

[00:31:47.44] They had a list of deadly items you can't sell on Amazon, and the list included things like flammable material that could blow up your house or pill-making machines that were being used to make drugs that kill people. And we showed that they were not only selling them but also talked to these people, like this fire chief, who was like, his daughter was killed in a fire by one of these flammable things, and he had personally been writing to Amazon repeatedly saying, you can't sell this stuff.

[00:32:28.87] And it was breaking Amazon's own rules, and there were just so many reasons why this was a low-hanging fruit. And literally

nothing happened, and then three months after the story, all of it was back up. This continues to happen. I mean, journalists are constantly writing this story. Amazon continues to sell deathly things that themselves they have said they won't sell, and there's no accountability.

[00:32:58.45] They just want to live in this world of we're just a platform, and we just don't have any responsibility for what we sell, which I have to say is just so-- it's so frustrating when you think about it. Because, as a journalist, I'm liable for every word we write, and we get everything checked by lawyers, which costs a fortune.

[00:33:19.82] And then we have to get media liability insurance, which costs a fortune and is impossible to get. And thus, fewer and fewer insurers want to offer it. And so for me to be held so accountable for every little thing, and then these giant companies have complete impunity. I mean, I know I'm not telling you anything you don't know, but it's just incredibly unfair.

[00:33:42.23] SPEAKER: And hopefully, we can revisit that in some discussions of CDA 230 on panels later today. Something struck me which actually was not one of the questions I was going to ask you, but I think it plays into this a bit. A little bit of what's going on here is that you're doing this vast, data driven, mathematical journalism with the goal of producing evidence that can then be referred to by logical, reasonable people.

[00:34:09.56] And yet, several times through this, you've pointed out that the hook matters. The narrative matters. The meme-ification matters. And that seems to me to maybe be the hardest part of what you're doing, to take something that's so vast and evidence driven and math and turn it into the one sentence or the two words that's actually going to make it something that's easily digestible by people. So to turn that into a question, what does that process look like?

[00:34:42.89] Is it the, you go, and you do interviews, and you find the individual human story, and you say, ah, this is it. This encapsulates what I took out of the math, or is it thinking about your audience, and what gets picked up on social media platforms-- possibly no longer Twitter-- and what the hashtag looks like. What is that process of translation from the big and the longitudinal to the small clip that's personalized and human?

[00:35:16.37] JULIA ANGWIN: That's the work. I mean, the thing that is the traditional work of journalism, and it is hard, but there are a lot of norms around it. And not all of them are good. I mean, I actually don't know that-- we do really want human stories, but the reality is that, particularly for these algorithmic harms, when we knock on the door and tell someone, our math says you're harmed by an algorithm.

[00:35:44.69] They're like, that seems bad. It's not the most compelling human story, but it's all we have to offer at the moment. Because the

problem is you don't know. That is the whole thing about algorithmic harm. We never could show that there were housing ads that weren't shown to Black people because how would you be able to prove that.

[00:36:06.56] It's hard to prove a negative, and so the world that I operate in is a particularly challenging one for narrative. And yet, the reality is, humans just love stories, and so there's really-- we do just knock on a lot of doors, and one thing about journalism that I was just telling young girls the other day, was like, it's just a huge amount of rejection.

[00:36:33.77] It's so much rejection. You get 30 people say, no, I'm not going to talk to you. For anyone that says yes, and of those, not all of them are even at all related to the topic you want to do. So it's a huge amount of work, but it is, like you said, the most important. I don't know if I want to say the most important part. All of it's important, but it's what gets you across the finish line.

[00:36:56.57] SPEAKER: Yeah, yeah, and I'm also hearing other elements of this that are about to bring up something from the first panel about amplification, and the role of not just different online platforms, but also different journalism companies in choosing which of those stories to pick up and amplify. So the second set of questions I had, which is appropriate because we're the law school, is about the role of the law in this.

[00:37:23.36] And I was reviewing your ProPublica reporting on machine bias, and noticed just how much open government law is there. You're reporting on an instrument that's built by a private company but used in government and much of the access was obtained through either filing for open records requests or going to the court system and seeing open litigation records that were available to you there.

[00:37:50.78] So what are the biggest practical hurdles and most frequent practical hurdles that you face when you're trying to get access. And I guess, I want to rephrase my question from, does the law matter, because I think I've answered it-- and plus, I'm self-important and a law professor-- to, how does the law matter? When does the law matter? When is it doing important work to get you the access to produce this kind of story, versus where is it missing where you think it could be?

[00:38:20.28] JULIA ANGWIN: Yeah, I mean, I've always thought of investigative journalism as having three legs of a stool that are, like, all three you need to do the work. And one is just incredible reporting. A willingness to talk to all the people, get rejected, still keep talking to more people. One leg of that stool is incredible legal support. You just really can't do serious investigative journalism without legal support.

[00:38:51.27] You need legal support for filing for public documents. You need legal support for-- what we did was collecting criminal

records from a public website. That was scraping. It's scraping public data, but there are places that would come after you for violation of terms of service. You need someone who's willing to defend you on that.

[00:39:15.12] The other piece of the stool that I think is really important is the engineering and data talent to do the analysis and make sure that you're using computation and automation, these great skills, to supercharge your investigative reporting. Because the reality is, journalists are outnumbered, outspent, outgunned on all fronts. And so I think we need to have every tool at our disposal, and I would say that legal backing is probably the most important one of those three. You really can't even get into the game without it.

[00:39:54.44] SPEAKER: Yeah, so I'll just, I guess, summarize the two types of law that I heard you reference. One is open government law, which is the meat and potatoes of traditional journalistic coverage of government entities. And we have somebody who'll be speaking on our next panel a bit about Colorado's open government law, and the kinds of access that it allows, versus the exceptions it contains.

[00:40:19.10] Then I heard you mentioned scraping, and the legal framework for scraping is the CFAA. And so that's almost an entire different category of lawyering, but now, with data journalism or mathematical journalism, that's part of the transparency story too. I've been wondering, because in some of the realms that I'm operating in, we're starting to think creatively-- we're starting to hope to think creatively-- about the use of other kinds of transparency rights that exist over the private sector.

[00:40:52.92] And I wondered the extent to which that might become a new sort of media law. So you think about these privacy laws, data privacy laws, that are being passed in multiple states, including our own, that include individualized notice requirements or individualized access requirements. Is there framing on the journalistic side of things that's thinking of like, hey, how could we use those points of access onto the private sector to do public interest stories that talk about the big picture?

[00:41:24.32] JULIA ANGWIN: Oh, yeah, I mean, this is something I'm very excited about, especially with California's access laws that are coming into play next year. The EU has got a whole bunch of more access laws coming out, and I know Colorado. And so those are the kinds of things where the dream is to get a lot of people to do public requests about their own data and then use all of those pieces together to try to understand what's happening.

[00:41:57.38] Because the challenge of the world we're in-- the world that we're in of algorithmic decision making is that you and I are going to get different decisions. We're going to get different things at the top of our newsfeed. We're going to get different decisions on which ads

are shown to us. We're going to get different all sorts of things. And so in order to understand what's going on, you just need a lot of data.

[00:42:21.69] This is why I started this national panel to analyze Facebook called Citizen Browser. Basically, I couldn't think of a way to hold Facebook accountable, and so without doing this, we've ended up doing a very expensive project, which cost almost a million dollars, to set up a national panel of users who installed a tool that we built that let us analyze their feed. And we saw their Facebook newsfeed. We stripped out the data that was personally identifiable, and they just told us things that they chose to self identify, politically, age, gender, race, geography.

[00:43:00.47] That was the only identifying details we use, and that allowed us to do a year and a half worth of investigative stories about Facebook showing that, repeatedly, they would make claims about how they were going to not boost something in their algorithmic recommendations, and then they would. And you need a huge panel of people to do that. Now, if people could donate their data, which is essentially what you're talking about, which is these give access requests and then donate them, that would also be another way to build this kind of panel.

[00:43:31.19] The challenge with the donations is that I have done projects like that in the past, and often, when you ask people to donate, the only people who are really motivated are usually your closest readers. And they don't always represent the full swath of the type of people that you would want to hear from to get a real representative view, which is why I ended up having to pay people to install this tool. But that said, it's better than nothing, and it's a great start.

[00:44:02.75] SPEAKER: Yeah, I'm hearing a theme both with that and the 30% of acceptance versus 70% rejection of, your samples are really skewed in journalism. So the follow-on question to that, we talked a little bit, or we heard a little bit in the panel this morning, and I think we'll hear more again in the last panel this afternoon about some of the dangers of creating public accountability or public transparency requirements for private companies.

[00:44:33.00] And so one of the counterarguments that we heard to provide access over, say, content moderation policies for large internet platforms is that can become a way to influence the substance of content moderation policies. It can effectively implicate First Amendment interests and even possibly First Amendment law. And so when you're thinking about this through your perspective as a mathematical journalist, I imagine that, on the one hand, having more access to information held by these companies is delightful.

[00:45:10.85] And on the other hand, in the current political environment, how much do you worry about transparency being weaponized against journalism and whether the use of transparency to

govern internet platforms is a canary in the coal mine for what potentially could be to come for newspapers and magazines?

[00:45:37.55] JULIA ANGWIN: Yeah, I mean, that's a challenging question. I guess, I am always just going to be politically and temperamentally and professionally inclined towards more transparency. I think there are always going to be downsides, and I remember when I started writing about privacy at the Wall Street Journal, and a couple of my colleagues came and said to me, this is not good for journalists.

[00:46:10.37] If you push for privacy, we might get less transparency and less data. And you should really back off, and I hear what they're saying. And I do still hear that from journalists from time to time. But I think, in the end, when we're talking about tech platforms. Specifically, which is what I think you're talking about, where we're talking about the all-public discourse and political discourse in the world, and that's pretty high stakes. And so I think that transparency is always going to have a double-edged sword.

[00:46:53.92] People will make different types of arguments. But in the end, I have to believe, I think, as a journalist, I do have an optimism that is not borne out by the circumstances. I'm preternaturally optimistic, despite the fact that the world continues to show me reasons why I shouldn't be. And so I do really believe that-- I have this belief, just the facts that people will actually do something. And that's maybe naive, but it is my driving force.

[00:47:30.56] SPEAKER: So I have two more questions just to suggest to the audience that you start teeing up questions to ask. My first actually goes a little bit to what you were just mentioning of your coverage of privacy and the response you received about this will be bad for journalism. Let's say you hold the pen for making a law, and you decide that you're going to skip through these oblique ways of trying to get access to information that these companies have.

[00:47:58.12] And instead, you actually are able to write a private sector FOIA. You write an open government law, but it applies to the private sector. What might that look like, and what limitations would you want to place on it based on the other part of your experience of covering privacy and seeing the implications of this for individual rights and dignity?

[00:48:23.78] JULIA ANGWIN: Oh my god, I mean, seriously? That is the dream. I can't even dare to dream. It's so hard to even get government FOIA responses. Private FOIA would be amazing. I think top of my wish list is stuff that is-- the way I view it is in terms of public interest and high human stakes. And so, for instance, I think that hiring algorithms.

[00:48:50.29] Those that decide whether you get a job or not through an automated system are so important. That is people's livelihoods

being judged by machines that are unaccountable, and we don't know are they compliant with employment law. Is it discriminatory? There's no testing of it. There's not really any way. And so those are the kinds of things where I think you can make an argument that there's a public interest.

[00:49:15.97] There's high human stakes, and there's existing laws that you would want to know that cover this area. And so that's just me off the top of my head saying the things I would think would be the criteria for this. I am not a lawyer. I do not write laws, and so I would want to consult with some people.

[00:49:34.96] But I would say that is something that would be amazing because I think-- I really, really worry about a world, which we're already in, where there's essentially a racialized underclass that is ruled by algorithms and automated decision making. They are hired by an algorithm. Their daily life is overseen by it. They're fired by it, and they can't get out of this system. And it's preposterous that we allow this to happen, and it is only going to get worse.

[00:50:09.99] SPEAKER: With that optimism, I have my last question. Yeah, tech policy conferences are always an upper. My last question is, I think, riffing off of something that Daphne did on the first panel today, which was she talked about the shift in the conversation over platform transparency from, say, 10 years ago from really being about accountability for government and trying to give oversight about government surveillance and government takedown requests to now really being about accountability over platforms.

[00:50:45.84] And I wondered if you could talk, since we're now approaching the 10th anniversary of Edward Snowden's leaks, about that arc as a backdrop to the work that you do. Have you seen a similar shift of the Snowden leaks highlighting government behavior to, now, a shift to looking at private actor behavior? Has it really all been part of the same story of complacency and jawboning and interaction between these companies and government? What are your thoughts on that 10 years ago versus now?

[00:51:25.77] JULIA ANGWIN: It's such a good question because, as a person who has covered tech for decades, grew up in Silicon Valley, and I think probably is considered a tech critic, I actually want to say that the tech companies, even to this day, are doing some heroic work resisting government requests. Particularly, in countries like India and repressive regimes where they want to use this information to crack down on dissidents.

[00:52:00.63] And so it is a double-edged sword. They are trying, in some cases-- I think Twitter was doing quite some heroic stuff in India recently-- to hold the line for free speech. And I think that that's something that has to be commended, and that's one of the things that's so difficult about the tech platforms. Because in one way, we want them, the beauty of them, transcending all of the laws of every

nation is this great promise that you could over ride authoritarian regimes with this unstoppable force.

[00:52:38.97] This is the dream of the early days, and then the reality is that once you have a global, corporate superpower that is unregulated by any government, that's also a problem. And so I think we've reached that point, where it was like, before, they were a little bit more scrappy fighting for us against government surveillance. And now, we realize, oh my gosh, they're the government.

[00:53:06.51] I mean, not really, but in some ways, they can choose who the election is. If Facebook wanted to just turn off all Republican advertising or all Democratic advertising, they could. They literally could, and so I hope they're not going to, but we are at a stage where their power is so massive that it makes sense for us to look at them in a more skeptical and more wary way than we were in the past.

[00:53:35.67] SPEAKER: Yeah, I think it was Kristen Eichensehr who refers to tech companies as digital Switzerlands. They're not of a country in that they are influenced by geopolitical power. All right, so I think my time talking is done, and I turn it over to our audience. And again, we invoke the Phil Weiser rule to start with a question from a student. Blake is trying to point at Richard. Yeah.

[00:54:06.83] AUDIENCE: Sorry, yeah, my job is just to deliver the microphone, but I can ask you a question too. Thanks so much for talking with us today. I really enjoyed your presentation. I'm curious your thoughts on the business influence of journalism right now. I mean, obviously, content moderation decisions are, regardless of the doublespeak, motivated by profit. They need to figure out what's best for their bottom line. How do you feel that journalism today is influenced by money?

[00:54:43.32] JULIA ANGWIN: Oh, well, because we have no money. So this is the problem. So journalism in the US has gone from a \$30 billion a year revenue 20 years ago to \$10 billion that's a huge drop. This industry is cratering. It literally is cratering. As a for-profit, revenue-generating business, which is why I started a nonprofit, and that's great.

[00:55:14.61] But there aren't a lot of billionaires out there wanting to fund nonprofit journalism. And the reality is you have to attach yourself to a billionaire. So I happen to have a nice one, Craig Newmark, but the reality is, that's the world. And that is messed up. There's a crisis in journalism, and what it means is that we're, as an industry, rather weak. A journalistic outlet is going to take the cautious move because they don't want to lose their media liability insurance, or their lawyers are going to say, you know what?

[00:55:53.66] Just don't take the risk. It's not worth it, and so what it means is journalism as a whole, and I'm not naming anyone specifically but as a whole, become more cautious. You have to. That is the

business imperative of an industry on decline, in a massive decline. With future revenues constantly plummeting, you're going to be risk averse. And so that is a problem for not just journalism but for democracy.

[00:56:21.14] SPEAKER: I have a question over here from Eric Goldman. We're coordinating microphones. Give us one second.

[00:56:31.94] AUDIENCE: Hey, Julia. It's Eric Goldman. Nice to see you.

[00:56:34.31] JULIA ANGWIN: Hi.

[00:56:34.85] AUDIENCE: So I mean, I'll read any story you write. You, obviously, are at the top of your game, but not every journalist is as good as you. And I want to talk a little bit about some of the risks that poses, especially with what you're defining as mathematics journalism. When I heard that, the first thing I thought was lies, damned lies, and statistics, that most of the people who are going to be trying to do what you do won't do it as well.

[00:57:01.35] And many of them, especially as you talked about getting rid of objectivity, will actually have a normative agenda to try and use statistics to show whatever they're trying to advance. What are we going to do about that? You've already solved the problem for you because you built these really industrial-grade systems. But what are we going to do about the rest of the people who can't do what you do?

[00:57:26.59] JULIA ANGWIN: I mean that's a great question, Eric. And I think it has to do with the structure of journalism. It's just, I think we have to admit as a society that journalism is essential to democracy, and we have to think of a way to save it. I think that the idea of taxing companies, using that money into some sort of fund that supports journalism is a good idea.

[00:57:55.51] I'm not a huge fan of these plans where the journalists all have to arm wrestle with Facebook for licensing fees because that feels very weird to do, especially for a small newsroom like mine. But I think that it's hard to build quality inside of a cratering business that is dependent on clicks, and so means the journalists have to write seven stories a day.

[00:58:23.08] Yeah, they can't do statistical analysis. They have to write so many hot takes to get those clicks to get that very pennies of ad revenue for those behaviorally driven ads. Now, I would say there's one thing that would fix some of this, which is not having behaviorally driven ads. Because the fact is that back in the day, advertisers wanted to advertise next to quality content because that's where they felt the quality of readers were.

[00:58:49.27] And those quality readers are still there, but they can find them cheaper on some other website because they track them. And so

I know this is heresy, but I still think we could sort of address this by saying, is it worth it? Is it worth it to have all the ads following you around if it means that journalism is defunded and democracy is destabilized? I don't know. Maybe not.

[00:59:16.10] SPEAKER: Yeah, when I hear Eric's comment or Eric's question, I think of two things immediately. One is that you get into this endless cycle of auditing. You have the journalists auditing the companies and then being audited by other journalists and-- wow, auditors, that'd be a good career move right now. The other thought that I had, and this is mainly just trolling Eric from the mic, is, how about accuracy requirements? So any additional questions from the members of our audience? I see one down here.

[00:59:54.94] AUDIENCE: Hi, thank you, Julia, for coming. You mentioned earlier that you spoke to a group of girls about their journalism, and I was wondering if you see any trends in academia or in the education of future journalists to utilize statistical regressions or analysis? There's a lot of literacy in education that has to come with learning that skill, and I'm just curious if you see that as a trend that's becoming more popular.

[01:00:28.87] JULIA ANGWIN: Oh, I definitely do. I mean, I think I have a skewed view of it because I think people like that are attracted to me, and so I hear from a lot of them. But what I hear a lot is actually that a lot of statisticians, data scientists, programmers are looking for more mission-driven work and actually really excited about the idea of contributing in newsrooms.

[01:00:54.19] And a lot of newsrooms just don't know how to use them. Because the people who run them are not literate in that, they don't necessarily know how to best utilize that skill. And I think the real talent that I have brought is just that because I was a programmer and grew up in a family of programmers that I'm not scared of them. I know how to talk to them. That's literally my only skill is just I'm able to be biliterate in journalism speak and programmer speak.

[01:01:23.11] So I find a real excitement in the computer science community, in general, to participate in this type of work. And the challenge I have is finding journalists who can also communicate with them directly. And so that's teachable, and a lot of the journalists in my newsroom have started off really illiterate in all of that. And by the end, they're programming and super into it.

[01:01:47.63] And so I think it's totally learnable, and I think both sides benefit. Both the journalists and the data scientist both get more empathy for each other in the work that the other one does through these types of partnerships. And so I have great hope for it. But obviously, as Eric said, I'm essentially an outlier in the industry.

[01:02:08.96] AUDIENCE: Thank you.

[01:02:18.44] AUDIENCE: Hi, I just had a quick question, a quick follow up. So in our last panel, we had a little bit of a discussion on the role of platforms as educators in content moderation for users. And I know you mentioned that algorithmic harms tend to be really hard to humanize when you're going door to door and talking to people, and they have of a reaction like, oh, well, that sounds bad, I guess. Do you see any part of your role as an education role when you're having those conversations with individuals that might not recognize algorithmic harms?

[01:03:05.74] JULIA ANGWIN: Absolutely, I mean, I think journalists, in general, have an educational role, and I wish that I've had more time and energy to devote to it because I think that is our job. One of the things that I feel really strongly about is that our job is not just to uncover things, but it's to explain things that aren't secret. So some of the stories that we do are just very explanatory, and I've always done that throughout my career.

[01:03:36.31] Because I really think that, oftentimes, the way the world works is not well described and is actually pretty shocking. Broadband is a really good example. The idea that there are dozens of states where there are laws that prevent municipalities from putting in their own broadband because the telecom companies have lobbied to say that no one can compete with us, and so that no cities can offer-- in those states-- can offer their own cheaper, faster broadband.

[01:04:11.80] That's not a secret, but it's still really important to tell people about. And so I really believe that that's the educational role, which is like, here's just a fact that is out there that you should know about. And similarly, with algorithmic harm, I think that is also something that is important to educate people about. People have a little sense of it because of their Facebook feed. They're like, oh, I had a post taken down or something, or I saw something that I didn't want to see.

[01:04:41.51] So there's, I think, some level of education through content moderation has sensitized people to this idea. But there's so much more to be done. I mean, so much of the work that we've done at the markup has not been about big tech. We've written about mortgage approval algorithms, and how they're racially biased or written about tenant screening algorithms. There's a lot that-- basically, tech is just a layer that every industry uses to hide their tracks, in my opinion.

[01:05:12.79] SPEAKER: Yeah, so another theme I'm hearing emerge is the news, as things that are not new, so using explanations and using data that's already there. They're already there to really highlight what's already happening, instead of being drawn to the shiny thing. I think we have one more time-- time for one more question before we are all released to lunch.

[01:05:41.68] AUDIENCE: First, thanks very much for being here today. You talked a little bit about your identification within Facebook of the dropdown allowing people to discriminate against people based on an ethnic class. I was wondering if, in other cases, your team have tried to reverse engineer some of the algorithms that have led to discriminatory behavior, such as with the data about whether or not somebody is more likely to be recidive, et cetera.

[01:06:22.98] JULIA ANGWIN: Yeah, we do a lot of reporting on racial bias because it's endemic in all the systems that we end up looking at. So we recently did an analysis of broadband speeds and showed that a lot of companies sell one-- they have one price for broadband. \$40 to \$60 a month for a home broadband, and they'll offer it flat across a city.

[01:06:54.66] But the speeds that they offer are vary, and some of them are below what the FCC even calls broadband. So we looked at where are the neighborhoods that are getting the slow speeds but paying the same price as the neighborhoods getting the high speeds. Well, just take a wild guess what kind of neighborhoods were getting the slow speeds and which one were getting the high speeds.

[01:07:11.97] Well, the low income and Black and Brown neighborhoods were the ones predominantly getting the low speeds but paying the same price as the people in the richer neighborhoods getting the 200 megabits. And so we do that type of analysis quite often because a lot of this information is hard-- you have to join two different data sets. You have to scrape all the data from all the broadband providers about what they say they offer. And by the way, this was an analysis just what they say they offer.

[01:07:41.19] Not even what they actually-- we didn't test the actual speed. So it's obviously worse, and then overlay that with census data, and you see that there's a pattern. We did the same thing with predictive policing. We found a data set that this predictive policing company had left unsecured on a website, and we scraped it all, and it was 40 million predictive policing things where they said, OK, a crime is going to happen here in the next two hours, which is how they do their predictive policing.

[01:08:08.35] So we went and looked and saw what neighborhoods, do they sending these patrol cars into, and it was very rarely white neighborhoods. And so this is the type of analysis that we regularly do because it's really important to understand what-- we have a real history of structural racism in this country. And so what are the ways that we're embedding that into these computer systems. It probably, I would hope, inadvertently, but I think it's important to expose it.

[01:08:37.33] AUDIENCE: Right, but my question was more about, has your team gone in and trying to build or reverse engineer the algorithms that determine where they're going to send the police?

[01:08:49.73] JULIA ANGWIN: Oh, yeah, so I mean, I think reverse engineering and algorithm is-- it probably could be done, but I don't know that that's our role. Our role is to the impact on humans in the world. So we're basically saying, this is where you send your cars, and we don't have access to the algorithm, and we don't have access to the inputs.

[01:09:16.67] And so we would be making a lot of guesses and trying to show what that model might be, and that's important work. But I do try to steer clear of the speculative as much as possible. I mean, I'm OK with probabilistic findings, but I think that the reality is, just like anything else in life, you're responsible for the outcomes. You made a product, and this is the outcome. And so we are the people who are outcome focused.

[01:09:43.57] Here's where your outcomes were. You should explain to the world why that's totally fine. I think there are other people in the world who are better at building these predictive models and reverse engineering them, and I think that's also important work. I wouldn't say we would never do it, but it's just not sure how it fits into our mandate given that it's already takes us a year to do the outcome analysis.

[01:10:05.53] SPEAKER: Everyone, please join me in thanking Julia for joining us.

[01:10:08.55] [APPLAUSE]

[01:10:12.45] JULIA ANGWIN: Thank you all. This was so fun.

Panel: The Shapes of Transparency

<https://www.youtube.com/watch?v=-gFqHtv9y1w>

[00:00:02.09] MARGOT KAMINSKI: So thank you all for joining us again. It turns out now it's a beautiful day. So I hope you're all having a chance to go outside and wonder at the glory of the snow clad flatirons.

[00:00:14.21] I have the pleasure of monitoring our second panel on the shapes of transparency. And in some ways, with no offense to the first or the third panel, it's my favorite. Because this is where we're really going to dive down into the nitty gritty details of variations and how transparency might be designed.

[00:00:35.24] So when I think about this from a legal scholars perspective, I'm interested in hearing what shapes of transparency are best suited for what purposes, right? We heard from the first panel that it's really important to identify why it is you want to use transparency in the first place. This is a panel where we get to hear-- well, once you know that reason, what's your method. And what's your process. And what's your enforcement.

[00:01:03.80] So I have the pleasure of introducing our panelists. And I'm going to do the introduction in alphabetical order. But then they're seated by the order in which I'm asking them questions. So you're going to have to sort of visually jump around. And maybe you can raise your hand when I introduce you.

[00:01:18.59] And then the other thing I'm going to say is going to be a little different from the format of the first panel, is that I would love to hear our panelists jump in after each person presents. So these are informal presentations, as you know, but once one of you answers a question, if somebody else has a follow-on thought, absolutely feel free to add that follow-on thought before we go on to the next panelist.

[00:01:38.90] All right. So way over on the other side, there we have Jeff Ausloos, who is a senior researcher and data protection. For those of you who are not European that means data privacy expert from the University of Amsterdam.

[00:01:52.58] Right next to me is Rachel Johnson, who is a local legal initiative attorney for the Reporters Committee for Freedom of the Press. Back at the very other end of the panel we have Andrea, who is a former student of mine. So I'm extremely proud to have her on this panel. And she practices data privacy law, including counseling companies on the kinds of transparency requests I've referenced throughout the day, subject access requests.

[00:02:17.75] Then we have right in the middle Bryan, who is an associate professor and the associate chair of undergrad studies at the Department of information Science here at CU. And finally Amanda Shanor, is an associate professor of legal studies and business ethics at Wharton

[00:02:35.81] All right. So we're going to start today with a conversation with the Open Government litigator, Rachel who is sitting immediately to my left. Rachel is bringing to this panel basically the expertise and the kind of media laws that we discussed with Julia during the keynote. And can talk to us about those as example of what works and doesn't work in transparency law.

[00:02:58.25] So Rachel, from your experience litigating CORA, which is the Colorado Open Records Act alongside other open government laws in Colorado, what are their benefits? What are those laws' benefits and what are their limitations?

[00:03:13.01] RACHAEL JOHNSON: Sure. Well, thank you for having me on this panel. Like Margot said, I'm with the Reporters Committee for Freedom of the Press. We are a nonprofit organization that offers pro bono legal assistance to journalists. And I'm based here under the local legal initiative, but it's based in five states. I just had to get that spiel out.

[00:03:34.86] But as far as some of the benefits of CORA when I'm litigating some of these cases is, one it certainly holds the government accountable. There's no other law as I would say as strong as CORA. And that's modeled after FOIA, that ensures that there's accountability for the government for access to information that the public, and as well-- journalists as well are seeking access to.

[00:04:04.76] It's also an act that informs the public. Obviously a lot of reporters are doing really important stories and really important work after they are able to get access to records from government agencies. And this is local state government agencies. It could be anything like your local school board, it could be the governor's office, or the state legislature. Just the whole gamut of state and local bodies.

[00:04:34.40] The other good thing when you get into the nitty gritty of CORA is that it's a mandatory disclosure statute. So it's not narrow like the Colorado Criminal Justice Records Act. Under CORA usually the government has to disclose information or records to an individual unless an exception applies.

[00:04:55.95] And there's many more exceptions under CORA than there are for FOIA. FOIA I believe just has nine exceptions. And CORA has many exceptions. And that's usually the case for a lot of state laws. So there's a lot of good benefits in knowing that when you request information it is your information, and you should be entitled to it.

[00:05:16.54] And one of the limitations I think of course certainly from litigating some of these cases from a journalistic lens, is that if you're denied access to a record in Colorado, the only way to get access to it is to litigate. You can't-- there's really no appellate body or board that will review the denial from the government before deciding to release the record.

[00:05:45.54] You actually have to go into court and ask the court to give you access to this record. So as you could imagine, it can get quite expensive to litigate in court, to get access to these records. And I think that's one of the limitations for sure.

[00:06:02.88] MARGOT KAMINSKI: Thank you so much.

[00:06:03.85] RACHAEL JOHNSON: Sure.

[00:06:04.56] MARGOT KAMINSKI: As a follow on question, is there room in your experience to use open government laws like CORA or like the CCJRA or like the Colorado Open Meetings Law, to get transparency not just into government but into practices of the private sector?

[00:06:20.43] RACHAEL JOHNSON: That's a tough-- that's a tough question. We were talking about this a little bit earlier. And I think there's certainly a way that private companies can use CORA to get information. Because really anyone can use CORA to get information.

But when you talk about CORA, it's very specific to access to government information.

[00:06:45.11] So the way a public record is defined as any record that's made maintain-- made maintain or kept for use by a state agency or local agency in the functions of what they do every day. So it's very challenging to look at that from a private lens. Although I have had a couple of cases where the state government will use an outside vendor that is a private company to maintain certain information.

[00:07:15.96] Like Secretary of State's office has this tracer database where you're able to access campaign finance information, and a third party, through a contract with the Colorado State, Secretary of State's office, they'll contract with that private party to maintain that information. And if you do request that information, they're in charge of disclosing it to you.

[00:07:38.55] But typically it's just not a privacy statute whatsoever. It's more holding state and local bodies accountable.

[00:07:49.51] MARGOT KAMINSKI: Sure. And then I think the last two quick questions I had for you. One is could you talk a little bit more about your least favorite exceptions? So like what are the worst exceptions to CORA? And the follow on question of that is going to be, should CORA be a model for transparency laws targeting say the private sector?

[00:08:10.75] RACHAEL JOHNSON: Sure. So I have many exceptions that just not me. I guess they should not journalists a little bit more than me. But there's one exception. It's called the personnel files exception under CORA. And basically what it says is that, if there are any records related to the home address, other personal information related to an individual, like their phone number, some financial information.

[00:08:39.54] And then there's a section of it that says any information that's made or maintained in the employer-employee relationship. That is a very narrow exception. It primarily means that a government-- an individual could not get access to someone's personal identifying information related to those things. Your home address, your phone number et cetera.

[00:09:04.98] But a lot of agencies use this exception to bar disclosure of records that should be disclosed to you. Like if you want to get disciplinary records of a principal in the Denver Public Schools or an individual public official, they'll use that exception to not deny access to a lot of journalists and public individuals.

[00:09:34.45] The other exception that is really tricky is the sexual harassment complaints and investigation section of CORA. And that is really interpreted by courts as being very broad. And usually it prohibits disclosure of any information related to potential violations from government officials.

[00:09:59.58] And one example I use is Governor Cuomo of New York. He faced sexual harassment allegations and there was a report related to whether or not those allegations had any validity. And that entire report was disclosed, unredacted. In Colorado a similar case happened with an individual who was the president of the school board-- Denver School board.

[00:10:25.67] And reporters I was working with sought access to that record. And they were denied under this exception. Until that-- almost the exact same report, a lot of, I mean they actually got access to the report but there were so many redactions that they couldn't see anything. And the court basically held that any record of sexual complaints or investigations will not be disclosed. And it's so broadly interpreted that you can't get any information.

[00:10:54.35] MARGOT KAMINSKI: Great. I mean not great. That's awful. So I'm going to extrapolate a little bit from your descriptions of the law, to again say, look this is the shape of CORA, right? The shape of CORA is a journalist or somebody files a request, and either get, say here's your info or we deny it.

[00:11:16.53] And in that process there might be an identification of we denied under this particular one of 75 exceptions. And then one thing I heard you say earlier that I did not know that was interesting, was that the only way to then go after them is through court. Are there other open records laws in other states where there is a sort of appellate system that lowers the expense of challenging the exceptions?

[00:11:42.99] RACHAEL JOHNSON: There are. I mean actually a majority of courts or a majority of states do have that appellate level. I think Texas has this appellate level decision making. And I believe a couple other states that my colleagues are in. I want to say Tennessee and potentially Pennsylvania have that appellate access. I could be wrong, but those are states where you do have that board that we'll take a look at your denial before you have to litigate in court.

[00:12:11.24] And Oklahoma and Colorado have the same exception, where you have to immediately litigate before you can get access to a record if you're denied. So a lot of people are just negotiating with a custodian at that point saying, can I have a little bit of information? Can I have access to some of this? It's typically still just a challenge.

[00:12:34.40] MARGOT KAMINSKI: Yeah, so I guess in answering the other question that I had posed about, should this be the model.

[00:12:41.48] RACHAEL JOHNSON: I think CORA is actually a very effective statute. If it's used correctly and if the government follows it correctly. There's no funny business. So I think it is a helpful statute especially when you compare it to the Colorado Criminal Justice Records Act, which is so narrow.

[00:13:01.67] You're only going to get records of official action which are basically like arrest records or maybe records related to pro-- not prohibition but probate information. And any other record under that statute. It could be anything. It's up to the custodians discretion as to whether or not they're going to disclose it or not. So a lot, I mean, you can get an arrest record but you can't figure out if an officer has been certified or decertified, and what happened.

[00:13:32.30] And that's just a huge challenge, I think. So that model I would say no. And I think a lot of folks before I got here have been working on trying to make that a better statute. But CORA, I think it's doing what it should do except for a couple of exceptions.

[00:13:49.94] MARGOT KAMINSKI: Any questions or thoughts from other panelists before we move?

[00:13:53.09] AMANDA SHANOR: I have a question about weaponization to follow on our earlier panel of transparency. So I have some friends in a Southern state who work at a public University and they've been subject to what they feel like at least are harassing FOIA requests, regarding their efforts to try to take down-- I think it's take down Confederate monuments.

[00:14:16.82] But sort of like that have blossomed into other things. I wonder if that's something that you've seen. I also wonder-- we have a colleague David Posen who has written an article about the ideological drift of transparency and how it's sort of like increasingly used for-- he says neoliberal kind of like corporate purposes as opposed to public purposes. Like do you see a lot of companies doing things to try to get their competitor under CORA or these things not?

[00:14:45.50] RACHAEL JOHNSON: I hope I'm answering your question correctly. Maybe not as-- maybe not as much. And this-- and this could relate to what you're talking about. There is this kind of new effort maybe along the lines of people seeking to ban certain books in libraries.

[00:15:03.95] AMANDA SHANOR: Right, exactly.

[00:15:04.64] RACHAEL JOHNSON: Right. So I had a reporter who sought access to these requests for reconsideration forms, which are basically forms that allow an individual to go into the library and say, I want you to ban this book. Like I don't like this book, please take it from our shelves.

[00:15:20.06] The problem is that the individual who requested the removal of the book, their name was redacted. And there were several individuals who were trying to ban this one particular book. And the reporter was trying to report on that because nationally there's been an issue with people saying we don't like Critical Race Theory, we don't like Gender Queer. That was the name of the book. We want that out of the library.

[00:15:46.70] And so that's certainly-- CORA is certainly making it a little bit difficult for our journalists to get access that way. I think that's-- I think that speaks to your question.

[00:15:57.59] MARGOT KAMINSKI: To Amanda's point about the weaponization of open record laws, the other person writing on this is Margaret Koka-- Margaret [? Koka. ?] Sorry if you can't hear me-- the mask, who has also similarly said FOIA, the Federal Open Government Law ends up becoming a way for companies to basically flood regulatory agencies with information requests and gum up the works.

[00:16:23.24] So there's the weaponization of, you use it against the University professors who are subject to open records laws to uncover their emails, to figure out what they're doing. Don't do that to me. No, it's all good. I've been subject to these before. And you have companies that are thinking strategically about how do we use the information that regulatory agencies are gathering on our competitors or how do we gum up the works at a regulatory agency to try to slow it down?

[00:16:52.73] So I don't want to make Rachel say the dark side of the open records laws. But that is the language around that. All right, so I'm going to turn next to Amanda. Amanda, you have written about the constitutionality of various disclosure regimes. And I know we will probably be hearing about this more from Eric on our third panel as well.

[00:17:13.49] From securities regulations to disclosures about deceptive marketing, what are the possible shapes in your view of constitutional mandatory disclosures? And does the First Amendment place any legitimate limits on what mandatory disclosures from companies should look like?

[00:17:31.58] AMANDA SHANOR: Awesome. Thank you. Thank you all for coming. It's really a delight to be here. And thank you for organizing. This is fantastic. So I thought one to tell you I have-- we're very high in the air, and there's very little air. So that may affect my presentation. So I thought to answer what I think is a really big and important question, and one that's increasingly being litigated today.

[00:17:55.85] That it would be helpful for me to lay out the First Amendment law around mandatory disclosures. A little bit about how it's changed over time and what the current dynamics in the courts are as a backdrop to my answer, about what kinds of disclosures-- mandatory disclosure should and shouldn't be constitutional today. In part because I know we have maybe not all lawyers. We have some students.

[00:18:19.10] But a couple of points before I get to that. The First Amendment debate I think is often both blunt and confused with policy questions about what governments should do, not what the outer limits of what they could do. And also kind of like to Daphne's

earlier point, conflated with what platforms should do or can do. And I think we need to try to disaggregate those things to the extent we can.

[00:18:44.00] I'll also say real important questions, there's a number of cases, including the net choice cases which have-- essentially, Texas and Florida's disclosure for platform laws, we already have a petition on one of them. The other ones coming soon. I think certainly the Supreme Court is going to grant certain those cases. So we're going to get a lot of issues around this.

[00:19:05.47] And I also want to say we have to bear in mind the constitutional rules are not just about platforms. They're about all these different other forms of disclosure. So things like SEC disclosures, nutrition labels, drug interaction disclosures. You kind of like, you name it. The thing that says wash your hands in the bathroom.

[00:19:23.66] So it goes far and wide. And I'll say I'm sort of speaking to it with this-- we have to think about the broader context in mind, not just the platforms. So the freedom of speech, it says just the freedom of speech. That can be confusing because for a number of reasons.

[00:19:41.03] One, it's like everywhere, right? Everything we do could be understood to be expressive. And so-- but the First Amendment has never protected speech as such, or expression as such. Instead, it's sort of looked at different types of social relationships and institutions. So for example, there's a lot of stuff that you colloquially will call speech, that's not at all-- it's like there's no First Amendment question.

[00:20:03.56] So for example, you all have to file taxes. Do you think you have a First Amendment compelled speech claim to say no you don't have to file the taxes? No, that's ridiculous. Or things like conspiracy. That's--

[00:20:15.97] MARGOT KAMINSKI: [INAUDIBLE]

[00:20:16.85] AN: OK, conspiracy, right? I have a First Amendment claim, I get to conspire to do whatever. Or like I got a bad grade in a public school. Well, I get to write whatever I want to Professor, you get it. So there's a bunch of stuff that's like not even in play that's called uncovered. There's other stuff that we don't call speech, but is covered like art or music, Mozart, whatever.

[00:20:36.16] So you get it. That it's not just all speech. And it really is sort of like there are different constitutional domains, I guess I'll say. Once you get into stuff that is covered, it doesn't all get the strongest strictest scrutiny, which I think sometimes people think there's only one first Amendment rule. There are actually many.

[00:20:55.87] So the most important one in play in these types of questions is there are sort of like big rules for political speech or speech in public discourse, and ones largely for commercial speech.

So I'm going to talk about those, because there's sort of like-- their interaction really goes to these, the heart of a lot of these things.

[00:21:13.58] So the political speech doctrine is mostly-- at least a gravamen of it is for democratic self-governance. It gets strict scrutiny. It's protected as an autonomy. Like for me as a speaker I get to say what I want. That means that government control efforts to stop me from speaking as opposed to-- and compel me to speak are treated the same.

[00:21:35.38] So like I can't say don't vote for Trump. They say I can't. Or they say, you have to say the Pledge of Allegiance. Those get the same kind of constitutional treatment because it's about what I can say. Commercial speech by contrast has been protected because of the informational interest of the public. So it's not about me speaking, it's about your hearing.

[00:21:52.57] And the court said-- why is this important? It said for two reasons. One, because people need information to decide-- commercial information from these transparency things to be able to decide how to vote, but also to decide how they want to interact in the economic world. And in a world in which we have a market economy, how each of us does things will affect these big questions. Like do we each wear masks? Do we smoke cigarettes? Do we use fossil fuels, et cetera.

[00:22:23.05] There's also an idea in the cases that it's about our ability to live freely in economic life. Our ability to get things like drugs that we need, to be full participatory people. So what does this mean? There are different standards for compulsions versus restrictions. Because we want more information to y'all, not less. So that means mandatory disclosures are treated with lot's of scrutiny than a restriction on speech.

[00:22:50.56] Also, it only really protects facts, not opinions. Because really what you want to know are facts that can inform what you want to do. So that's sort of like the baseline. Recently there's been a huge movement, which is called new lockdown by some people to try to weaponize-- to try to weaponize the First Amendment in a way to make it much more deregulatory and that's like an all purpose tool.

[00:23:16.78] So this is-- maybe even particularly the case in the context of compelled speech. So bunches of companies are like, you can't make me put on a nutrition label because I don't want you to know my dooghnut has 800 calories-- free speech. Or yeah, Exxon says you can't investigate what I knew about climate change-- free speech.

[00:23:37.18] I'm not kidding you. So courts have been struggling with these things. But I think really have moved in this very property protective understanding of free speech. And which to me meant that there's been less constitutional space for mandatory disclosures. I think

that-- so basically the First Amendment has become like a very strong all purpose deregulatory tool.

[00:24:04.01] That might be good, that might be bad in part, because anything can be expressive, right? So it can be used in many different ways. So that's sort of been the background trend to what's happening, but we have a new court with new people. So what I just said I think mostly applies to the Kennedy Court.

[00:24:21.92] And there's a question of what's going to happen now. And I think a really good one about whether or not the new court is going to focus more on the religion clauses, on the major questions doctrine, as opposed to really using the speech clauses as its central deregulatory tool.

[00:24:42.03] I also think that they still want to know about drug interactions for the heart medications. And they don't want to crash markets by shutting down the SEC altogether, at least. But maybe I'm optimistic. So this is sort of like where the background is.

[00:24:57.47] So then I'll really quickly say what do I think that means in terms of the space for constitutional mandatory disclosures. I think that there's should be a pretty broad space. But it should be oriented to these underlying purposes of why we protect commercial speech to begin with, which are a really democratic participatory purposes. So that we can have information to vote and to decide how we want to live and actually be able to live in our economy.

[00:25:29.90] And I think disclosures with those things in mind, that are factual and accurate, generally should be understood to be constitutional. What does that mean? I think a lot of data privacy disclosure should be constitutional. I-- what?

[00:25:41.60] MARGOT KAMINSKI: [INAUDIBLE]

[00:25:42.68] AN: Yes, totally. OK, I think that the SEC has new climate disclosures. I think those are constitutional. I think many forms of private FOIAs would probably be constitutional. But they're also really important limits to this. And I just want to flag I think the biggest ones.

[00:26:02.18] One is opinion, right? So the idea is to get facts to the public not opinion. So I think that you can't make a company say, yes I support this law. Or Republicans are great or whatever. That's not constitutionally permissible. I also-- there's also this idea of editorial discretion.

[00:26:22.55] And this goes to a question of like OK, how are we going to treat platforms or new types of media? Do we think of them more as looking like a newspaper or do we think the more as looking like a regular company that's being regulated to send stuff to the SEC? I think they're different.

[00:26:40.52] But I think the main thing is we need to not think about disclosures as one thing. But as like in a more line by line way, where what you do with a person doing it versus an algorithm doing it, we might think that that's a different question. The disclosure have to be factual and accurate. They-- and there may also be a question in terms of their implementation about state abuse.

[00:27:07.76] I think that that's probably best not get at through curbing transparency rules. But instead about trying to really regulate how-- whether or not the government is doing it with an untoward motive. So that's basically what I have. What I want to say, this is where I think the boundaries of the First Amendment are. Not what I think is advisable policy either for governments or for private companies.

[00:27:32.35] MARGOT KAMINSKI: Thank you. Around 700 questions, but I also want to be mindful of time. That was the most amazing-- amazingly succinct outline of extremely complicated case law that I've heard in a long time. So thank you.

[00:27:44.74] All right. So we will come back to this. Bryan, I want to turn to you next. So Bryan, your work and your lab's work on the role of technology in enabling resilience among people, particularly marginalized people, often focuses on platform design. And the ways in which the affordances of platforms, the sort of shapes of platforms play a role in enabling or preventing such resilience.

[00:28:08.02] So to target this through a transparency related question, what does well-designed transparency look like from a design perspective when you're talking about enabling your users to protect themselves in the way that you study?

[00:28:20.26] BRYAN SEMAAN: Yeah. So can people hear me OK with this mask? OK. So I also wanted to thank everyone for coming here. I'm going to start-- I kind of want to start this conversation with a bit of a background about myself and the work so that I can then situate transparency and context.

[00:28:35.99] And so just to give you a sense of my own personality and my identities that sort of brought me into the exploration of resilience as a phenomenon. So I am a first generation American. My parents fled the various wars in Iraq and so-- as refugees to the United States. Were members of the Indigenous population of Iraq. So does anyone here familiar with Assyrians, Chaldeans?

[00:29:01.51] That's what I am. We're not very well-- we're not very well known. But all of these experience, all of these experiences as someone in between these two social worlds of being an American and an Iraqi have given me the sort of experience of always been in between in this liminal state of trying to figure out what the heck I am. And how this world in this universe works.

[00:29:25.34] And so in those experiences, I went-- and I went and I trained as a traditional computer scientist who was learning programming and algorithms and all of that other fun stuff. And in all of that work I kept thinking and seeing more and more that technology was doing a lot of bad too.

[00:29:44.27] And so-- and so we often think of technology as like this thing that can save the world. But on the other hand, it's also doing a lot of bad. And so-- and so in that, my work really focuses on that relationship between where it can be, this very pro-social positive force in the world, but also this very negative thing that people are just experiencing by virtue of how it has been designed, constructed, created by whom it is being created for, whom it is being created.

[00:30:12.02] And so my work has focused very heavily on how people draw on technology as a resource to build resilience. And so in this-- by resilience I'm really referring to how people build resistance or bounce back from vulnerability or threat. And so in drawing on my-- drawing on my experiences, my initial sort of research in this area really focused on people living through war.

[00:30:39.38] And specifically the second Gulf War in Iraq and how they were drawing on technology to build resilience. And then over time my work started to focus on transitions and people who experience these life phase transitions moving to another status or condition. And so I've been looking a lot. So I looked at a lot at refugees, veterans, trans communities.

[00:31:02.54] And then more recently, my work for the past decade has really focused explicitly on those at the margins, and who are made vulnerable just by virtue of being born Black, Latinx, queer, et cetera. And so in that work-- in that work and-- in my work and in the work of others, one area that we've really started to hone in on in the context that's related to transparency is algorithms.

[00:31:31.97] And so when I think of algorithms I'm really thinking about these Black box systems or artifacts that underlie social-- technical systems, that shape a lot of our everyday experiences. So if you are using anything from Facebook to TikTok, there is an algorithm that is doing something behind the scenes that shapes how you experience that system. And also your day to day life.

[00:31:55.04] And so-- and so more famously like these algorithms can control our beliefs, our assumptions about things. Like they can determine who gets a job, how long people will remain in prison or who-- or how long for sentencing and things like that. And so as a scholar who reflects on transparency, more broadly through those experiences with people at the margins, I think it's really important to then talk about how the kinds of harm lack of transparency can produce.

[00:32:27.37] And so-- and a lot of this comes through how these systems are designed. So like when I'm thinking about an algorithm that predicts sentencing, there is a more famous example. Where depending-- so like-- so how many of you have seen this example in the more contemporary media that illustrated how these sentencing algorithms.

[00:32:48.70] When they are given to people, where one person is a white man who has committed more horrific accidents, say a Black man, it'll have a two year sentence requirement as opposed to a nine year sentence. And so these things often reiterate. They perform a very racist set of logics. But it's not very clear how those things work.

[00:33:13.64] And in my own work I've looked at a lot of this through two specific platforms. And so TikTok and also Reddit. And for a brief moment, I want to talk about in the context of how Reddit is perpetuating harm through this lack of transparency. Or sorry, how TikTok is perpetuating harm through the lack of transparency.

[00:33:34.67] My grad student colleague and I, Ellen Simpson, conducted a study looking at LGBTQ+ community members and their use of TikTok. And through this study, we were talking to people about how they are experiencing the platform. And if you're not familiar with TikTok, TikTok is a For You page, which is mediated by an algorithm. So an algorithm called the For You-- For You page algorithm.

[00:33:59.38] Really tries to learn about the users on the platform. So through your clicks, through what you're watching, through what you're engaging with, it will then present material to a user. And it really tries to put people into buckets. And so on the one hand, it has representation.

[00:34:16.87] So there's representation. There was queer representation. People were seeing themselves reflected in a lot of this material. But then when you start to intersect different identities, what we started to see more and more is that you could be queer, but you can only be a very specific kind of queer.

[00:34:33.10] So you could be a White-- you could be a White woman lesbian but you could not be a Black woman lesbian. Because the content and the videos produced by Black women was being erased. And so through some of the work that we-- when we started talking to some of the designers, we learned that they actually had very specific criteria that was given to them as policy by TikTok, which--

[00:34:57.31] This is verbatim. I'm not making this up. It said if people are fat, ugly, Black, et cetera, you should remove those videos. And this was-- we started studying TikTok when it really started to make the mainstream here in the US. And so on the one hand, I can say a few big tech, like you really piss me off.

[00:35:20.64] And as many people should be questioning a lot of what big tech is up to, I also think that we have to couch our response in the context of what I'm referring to as like a transparency cost, because when we're getting into-- when we're getting into how design is accomplished in formal settings, like making things transparent actually is oftentimes in conflict with the incentive structures of industry.

[00:35:52.94] So like who-- so like let's say I want data to go and understand transparency, or like the lack of transparency at a corporate institution. Who's actually going to generate that data for me where is that going to come from. So like what structures really exists around that.

[00:36:11.01] And so-- and so I think-- and I think the other thing that I want to mention is even in situations where as a computer scientist and understanding somewhat how algorithms work, people who study neural networks as an example, even if they have full control over all of the variables, they ultimately don't know why those neural networks present what they do.

[00:36:34.22] So like even transparency, the design level and the creator level is very-- it's not that clear. And also-- how much time do I have left, I should ask.

[00:36:44.05] MARGOT KAMINSKI: Three-ish.

[00:36:44.39] BRYAN SEMAAN: Three-is. OK. So I think-- so I think I wanted to kind of situate that transparency across in two examples that I think are very important. And I'm going to come back to dating apps for a moment. How many of you have used a dating app? Right.

[00:36:59.65] And so I was at the office. So I often attend a conference called the SIGCHI. It's the human-- it's the human computer interaction conference. Which is like a big design conference in my community. And one year we had the pleasure or the displeasure of having a keynote given to us by one of the co-founders of OkCupid.

[00:37:22.99] And in this talk, the founder of-- one of the co-founders of OkCupid was describing how they're using data to read, to constantly evolve the interface of OkCupid. And so initially when OkCupid started, it was much more like a match.com interface, where it was more about depth of a profile.

[00:37:45.38] And you could go and learn about somebody before swiping left or right. And they saw over time that most people were spending a few moments on a profile and just making a decision. Which led them through that data-driven perspective to believe that people were only basing it off of looks.

[00:38:02.88] And so they decided to then reorient and restructure their entire interface around that premise of left and right, you know,

swiping. And then this is where it got super disgusting. He made the comment that, we also learned through that data-driven analysis that White men did not like Black women. And that we eliminated all Black women from this field of White male-- from the feeds of White men.

[00:38:31.88] OK, so that's like-- that was like pretty devastating. And there was a huge uproar at this conference. And this is a case where transparency becomes increasingly important. Like making that kind of data and those decisions and the values available to people, so they can understand how that is being implemented.

[00:38:51.14] But another case of a dating app-- and I can't speak to this because it's from a study. And so I'm going to call it from Platform X. And so Platform X as part of their design, they needed to-- they were really thinking about-- well, in a dating app you're really trying to get people to establish a meaningful connection as opposed to a hookup app. And so they're really trying to create a dating app in this case.

[00:39:13.97] And what they ended up talking about was they were using the metaphor of a bar. And they wanted to-- and they said when people go to a bar, you stay at a bar for a while and you might interact with some people and you might miss out or what happens. But you're there for a while.

[00:39:29.92] And so they're really thinking about this engagement around keeping people sustained with the platform until they found a meaningful connection. And one of the ways in which they're implementing that was they said they started to assign people with beauty levels. And depending on their beauty level they would always show people like other people to them that were above their level, so to speak. So that they would maintain interest until they established a meaningful connection.

[00:39:58.10] So that's just more of like a provocation of like, do I want to know what my beauty level is? Probably hell no. But there's some-- so I don't want to know that. So this is kind of getting into this. This really illustrates the complexities of transparency in the context of design.

[00:40:17.93] And I really believe that in order to realize this goal of transparency and the design process and the design context, it really has to become a value that's integrated into that process from a-- in a very formal way. And so it's going to really require a transformation because oftentimes a lot of technology is designed outside of policy.

[00:40:40.58] And so I think this has to be a larger holistic collaboration between policymakers, designers, law et cetera, while also taking into account the costs of transparency. And we should be asking questions around transparency for whom transparency, when transparency, at what level.

[00:41:00.62] And these-- and the policies should also empower people. And so I really think that part of this is in my class. And I'll end with the final-- in my classes, I teach a lot of design courses. One of the things that I always championed is that if we actually had-- if we actually gave voice and agency to people at the margins, and actually having a real active discourse in how things are constructed, that the world would be a better place.

[00:41:25.30] MARGOT KAMINSKI: Thank you so much. I know this is a live conversation in the field of algorithmic accountability in terms of how to legally structure potentially that kind of stakeholder and impacted individual engagement. So definitely excited to talk more about this. To my two subject access requests people, I'm going to ask you guys to each try to do around 7 minutes so we can get to discussion.

[00:41:49.30] First, we have Jeff. Jeff you're working in European Data Protection Law, and you've done this work on subject access requests, disclosing how individual transparency rights can work sometimes. We heard this in the conversation with Julie-- Julia. On shedding light on bigger societal and governance problems.

[00:42:07.06] So what are subject access rights? What are the limitations? And how might they be improved potentially as a tool to get oversight over the whole system as opposed to just oversight for individual people?

[00:42:20.63] JEFF AUSLOOS: Right Thanks, Margot. Can everybody hear me like that? I take a bit of a distance, yeah. So first of all, thanks for having me over. It's a great discussion so far. I enjoy the panels and the keynote a lot, especially coming from Europe to get more of this American perspective.

[00:42:38.42] But I'm here, as I talk in European, so I'll be giving more of a European perspective. And so for my intervention, I really want to talk about or focus on the positives of these data access rights in the GDPR. And increasingly also in other legal instruments in the EU. And how they are challenged in practice.

[00:43:06.60] But perhaps first let me take a step back and very briefly look at the GDPR, the General Data Protection Regulation as a whole, which is often framed in Europe, in the US as a privacy regulation. And I mean, some of you may know that one of my pet peeves is to say that is not the case.

[00:43:30.87] It's not a privacy regulation at all. It's really about infusing fairness, transparency, and autonomy into data infrastructures. And safeguarding all rights, freedoms or interests, as you are affected by these data infrastructures. And those controlling those infrastructures obviously.

[00:43:50.58] So concretely, this basically means that these data rights that the GDPR gives to individuals, right of access, right to erasure, right to object, right to data portability. They're useful for protecting my privacy sure, but also for protecting my free speech, non-discrimination, my integrity and so on.

[00:44:12.40] And there's a growing number of actual real life cases, real life initiatives where these rights are indeed used for these different purposes. So to better understand credit scoring algorithms, for example. Or to challenge all kinds of different types of recommender systems. Or to support workers' rights in the platform or in the gig economy context. Or indeed also to expose discriminatory practices in college admissions.

[00:44:40.53] So these are all situations where it's not really about the privacy of individuals, but more like exposing and challenging injustices. All right so looking at transparency and data access in particular now. These are themes that run throughout the GDPR. They are actually also parts of the Charter of Fundamental Rights in the EU. And they're also a recurring theme throughout this avalanche of recent EU legislation on technology. So I'm going to spare you the details on that.

[00:45:15.08] So in the GDPR, the key provision here is Article 15 on the rights of access, which gives you the right to obtain a copy of all of your personal data. And personal data is interpreted very broadly. And then some. So a copy of your data plus a whole bunch of metadata, which is often for about where did the data come from, who was it shared with, how long is it stored for, what exact purposes is each data point used for, and so on.

[00:45:45.85] And then there's a whole bunch of modalities that are specified by the GDPR. It should be easy to exercise, the information that comes back should be intelligible, it should be free of charge, there's a one month time limit and so on.

[00:46:02.28] A key feature that makes these access rights so useful is that they are intent agnostic. You don't need to motivate why you're exercising this right. And this makes them very multi-functional, especially when you're exercising them in a more strategic and collective manner.

[00:46:23.56] So for example to expose what I was talking about before. Is this systematic or a systemic issues such as discrimination? A clear example is in the gig work context. I can talk about that later in the Q&A if you want. There's been some big cases in the Netherlands against Uber and Ola, two gig work platforms on specifically using access rights to expose these algorithmic management systems.

[00:46:54.17] Now, one concrete instance where access rights also show a lot of potential and are increasingly used is in investigative research. We've seen the talk by Julia Angwin. So for journalists, but

also, of course, for academics. Because from talking with a lot of social scientists, especially researchers are increasingly struggling to observe the world around them, as it's increasingly digitized and privatized.

[00:47:24.01] And so if we want to understand education, work, transportation, social practices, we simply need to be able to observe the digital infrastructures on which that these things are largely taking place today. And so the impact of lockdowns on dating life or working habits or the impact of political micro-targeting on polarization, these are all issues that we need access to information-- to data for.

[00:47:53.82] So to me, these data access provisions, this discourse is not just vital to hold platforms accountable. It's an important component. But it's increasingly also necessary to just understand society and to do science and journalism.

[00:48:08.94] So yeah, a brief point also worth mentioning is that this emerging work on so-called data donations and was also referred to by Julia, there's really a growing field in Europe, especially where people can agree to give some of their data under certain conditions to researchers.

[00:48:30.71] All right, so briefly now I'll talk about the issues and challenges. Specifically there's quite some challenges with the interpretation, application, and enforcement of these access rights. And so first of all these access rights are formulated in a very broad and vague manner. And the reason for that is that it's useful for a very broad and wide applicability.

[00:48:56.14] The flip side of that is that it pushes interpretation costs downstream. And this means that in practice, already powerful actors, whether it's industry or government bodies, they very much set the tone on how these laws are interpreted and applied in practice.

[00:49:12.10] And this is evident time and again. I've done plenty of empirical research projects over the years on looking at access rights compliance. And time and again it's very clear that there's a very narrow interpretation and application of these provisions in practice. And so this vague phrasing also is very far removed from the practical realities, where these rights can be most valuable. And I very much appreciated your talk just now Bryan.

[00:49:43.08] People that arguably need these rights the most, that are most impacted by these data infrastructures, like marginalized communities, exploited workers, asylum seekers, any kind of vulnerable person that is affected by these digital infrastructures, they generally have no real meaningful access to these rights.

[00:50:03.41] And so the coordination of these data rights may help overcome to some extent the accessibility of these rights. But raises a whole bunch of concerns and questions to who is the coordinator, is it

a for profit entity for example, what happens to the data if it is pooled, how are the identities of individuals verified and so on.

[00:50:26.43] And then there's a whole bunch of enforcement issues that I could get into, but let's keep for the Q&A, if there's an interest.

[00:50:34.82] MARGOT KAMINSKI: Thank you so much. So finally to Andrea. You're the other side of the coin on the subject access requests. You get to tell us what goes on inside companies when they receive these things. The good, the bad, and the ugly.

[00:50:49.25] ANDREA MACIEJEWSKI: Yeah. Now, so thank you for having me. I'm very honored to be the company side of all of this. And I take that not lightly at all. So before I actually answer the question, I think some background is in order, and some of my own observations working with dozens and dozens and dozens of companies over the past years.

[00:51:10.04] I think when we develop privacy laws and we talk about privacy, oftentimes we are posing the corporation as the big evil. So they're doing all of these bad things. They are misusing data. There are horrible things. I do not disagree that there are bad actors, absolutely. There are companies who are doing things with data that should have never been done in the first place.

[00:51:33.05] But I have never once worked with a company who were on a condo like hey I have all this data, I'm so excited to use it incorrectly. Most of them are honestly trying so hard to do the right thing. But we're all fighting an uphill battle here. Because the CEOs, the board of directors, the people with the money, they haven't jumped on the privacy bandwagon.

[00:51:58.58] So what's happening is we have all these huge laws that are really complex, that are multi-jurisdictional, coming in and you have to do all of this stuff to do the right thing. And there's no money. There's absolutely no money. There's no resources. So they're under-resourced. They're under budgeted.

[00:52:16.55] And I think that plays into the transparency aspect. Because in order to effectively respond to an access request, there is so much that has to go into it. A company needs to first of all have a perfectly clear and absolutely crystal clear view of their data. They need to know what data do they have, where is it, who is it shared with, when is it used, why is it used.

[00:52:44.37] For big companies who have been collecting data for many years this is no small task. This isn't like looking at three or four spreadsheets. This is looking at multiple countries, multiple databases, multiple people's file cabinets, which isn't a bad thing. I think that all companies should do this. And this is step one.

[00:53:04.65] But that's a project that costs no less than \$50,000 for a small company. I've seen it go up to a half a million. And when you're talking about companies that don't have a budget, that's a big chunk of change to do it right. OK, so we've got this fine. Let's have our hypothetical company have a perfectly clear view of all of their data.

[00:53:27.46] Now, they have to sift through the data and start pulling out the things that shouldn't be disclosed, maybe because there's third party implications, maybe because there's trade secrets. Perhaps there's some data that is actually going to pose more risk to the company than it would be to not comply, which isn't necessarily the right thing. But it's a reality.

[00:53:46.59] Like we're all talking about business risk here. Am I actually airing my dirty laundry so that I can get sued for employment discrimination, which again isn't necessarily a bad thing that they should be transparent about that. But is that the reality of what you're getting going back to the interpretation of corporations?

[00:54:05.28] So we've got all of these hurdles that we have to get through. And then at the end, we have to produce something to the requester. And part of the difficulty that companies are facing is what is the purpose of these requests. Like if I go to Acme corporation I say, give me all the data that you have about me. Why am I asking for this? If it's a fishing expedition or a research expedition OK, fine. Like you actually do want a spreadsheet.

[00:54:32.82] But like as a consumer, do I really want 400 pages of metadata? What am I really trying to understand here? And so I think on a personal level, one of my issues is that many governments, AGs, people who are passing these laws pose it as this is good for the consumer to control their data.

[00:54:55.39] But what am I controlling when I'm putting forth an access request? If we're being honest about it, it's a way to hold companies accountable. It's not for me necessarily to understand what data there is about me. It could be, right? Maybe I do want to know what I bought from the grocery store five years ago on April 2nd, I don't know maybe.

[00:55:15.97] But am I going to find that in the 400 page document that I'm getting back? I'm not sure. So I think to answer your question, transparency from the corporate side is the right way to go. But we've got a long way before we can get there. And unfortunately enforcement is coming faster than we can get the money to get it done.

[00:55:37.13] And so that's why companies are concerned. They want to do the right thing, but they can't in many cases.

[00:55:46.37] MARGOT KAMINSKI: Thank you so much. So I think at this point it's appropriate to open up to questions from you all. And

also to from the panelists to each other. So if you want to raise your hands, I will call on you too. But once again, the filibuster rule rules. And do I have a student who would like to start us off? [INAUDIBLE]

[00:56:04.26] Oh, hold on a second. We need to get you a microphone.

[00:56:12.65] AUDIENCE: Hi, thanks a lot for this amazing panel. My question is mostly directed at Andrea. Given the difficulty for companies to actually come up with this perfect system whereby they can implement all of these rules and still be profitable, and they don't want to air out their dirty laundry accidentally whatever, how do we strike the right balance between transparency, consumer rights, and sort of like profit?

[00:56:47.97] MARGOT KAMINSKI: Just a small question, Andrea.

[00:56:51.51] ANDREA MACIEJEWSKI: If I knew that maybe I'd be a governor. But I think it's a really good question and something that the market is trying to figure out right now. So we do benchmarking and we look at what all of the different companies are doing. What types of documents are you getting in response to access requests.

[00:57:08.65] So if you survey 40 different companies, what are you getting back? And we see it all over the map. I think the interpretation comment is spot on. We have some companies who are giving you one page responses, with only the stuff that you know you've submitted. Write your name, your email address or phone number. And I'm like, great I know you have more than that on me.

[00:57:26.80] But then I've also actually seen a 300 page excel spreadsheet line by line that is absolutely unintelligible to anyone except for like an aerospace engineer. And I think what we're going to see is two things. One, the market is going to start to center and hone in on a specific way of treating access requests.

[00:57:49.74] And I think that we will see regulators come in and give guidance on whether it is or is not appropriate. We have a lot more guidance from Europe than we do from say California obviously, any of the new states. And then I think the second thing that we're going to see is more-- we're going to see more automation, more technologies come in to help companies get there.

[00:58:10.80] Because right now a lot of this is manual. Like you have a three-person IT team and a two-person marketing team. And together they are trying to cobble together some access requests for a law that, frankly, they don't understand and never could because it's too complicated. So as you get more technologies that do understand the law, they understand what has to happen, that along with the market centering, I think will give us a more clear path forward.

[00:58:39.43] AUDIENCE: [INAUDIBLE]

[00:58:40.14] MARGOT KAMINSKI: An interim question. And then we have a question over there from Daphne. Which is, one way to potentially thread the needle I think runs into Amanda's First Amendment landscape. Which is instead of asking hey, hand over all the data, you say, tell me what it is that you're doing.

[00:58:57.27] Like produce this new information. It's not just the facts you have about me, but it's the explanation of what the algorithm is doing. And so I wonder both from a-- to both of you-- to each of you, and actually I guess to Bryan also. To Andrea, is that preferable from a company standpoint in its sort of efficiency or is it regulatory confusing?

[00:59:20.75] To Amanda, does that raise a different set of First Amendment problems than just hand over the facts that you have about this individual? And to Bryan, when you're thinking about transparency and its pros and cons from the perspective of a user, the tension and explanation is really how understandable is it to the user versus how useful is it actually uncovering the issues that you referenced. I don't have a preference on order, so any of you.

[00:59:51.27] ANDREA MACIEJEWSKI: So I was actually thinking about something very similar earlier when I was determining what I was going to say. And one of the solutions that I've always thought might be helpful from a consumer standpoint is to be like, I want this category of information about me. Because if I do want my receipts from the grocery store it would be so much easier to just ask for the darn receipts rather than get a 300 page metadata.

[01:00:12.72] But at the same time, my clients hate doing category requests. They would rather just produce all of the data, because it's very difficult for untrained employees. Because again, a lot of these legal teams are two people, and they have every other type of legal issue to work with. They can't discern what is a certain category, like what is internet activity, like what falls within it.

[01:00:38.71] So it creates more questions than it does responses. And so if we were to say like, what are you doing with the information? I think it would be really hard right now because it's-- the laws are so new and they're so complicated, that unless you are doing privacy every day, you may not even understand what the task is.

[01:01:00.72] You have to be so clear and the regulations would have to be so precise for that to work.

[01:01:06.09] MARGOT KAMINSKI: Yeah, I think you're going to stay up and Open Government attorney thinking like she definitely has an opinion about this. So I'm adding you to the queue also. So Amanda or Bryan?

[01:01:16.11] AMANDA SHANOR: Or also Rachael [INAUDIBLE].

[01:01:19.47] RACHAEL JOHNSON: I was formulating a response because-- go ahead, Amanda.

[01:01:24.21] AMANDA SHANOR: So this is on-- so your question is a really important one, because it's also coming up in the SEC context now about the climate disclosure rules. The idea is not just sort of like here are my statistics of how much carbon, but also here are my plans to try to deal with it.

[01:01:43.50] And is that a fact or is that an opinion? I certainly think it's fact. Like this is what you are doing. But the companies I suspect will argue that that's an opinion or should be understood to be an opinion. Or it's too speculative to possibly be a fact. And there are all these-- there are all these interesting hard and really important questions about how we should think about effectiveness, especially in the context of scientific--

[01:02:14.07] When we're talking about risks and uncertainties, or just normal accounting principles, all these things have built-in mathematical assumptions. Are those assumptions a form of opinion? If it's not 100% going to happen, does that make it opinion? I think the answer has to be no, if we're going to have-- just because the nature of science has some uncertainty baked into it.

[01:02:39.76] Otherwise, we're going to have environs who would we want the Constitution to be like, being the one deciding these issues. So yeah. So I think something like that, like what's are policy can be disclosed. But I think there-- especially when you get into the platforms and content moderation, at some point you're going to hit like is this editorial discretion in another way?

[01:02:59.29] But if it's not known to be editorial discretion, like I'm just manipulating people without them knowing-- the thing about a newspaper. You know what's a newspaper. It's going to give you an opinion. The thing of when you go on Facebook and you're like, they're moving you around, I don't know. So I'm inclined to think [INAUDIBLE] things are facty?

[01:03:14.37] MARGOT KAMINSKI: How facty is it-- facty being an official word derived at this conference. How facty is it and also like how transparent is the platform being about whether or not this is an opinion might actually be part of the legal construction of is it a fact. Bryan and then Rachel you are totally on queue.

[01:03:33.61] BRYAN SEMAAN: Because not to take up-- not to take up too much time. I wanted to very briefly comment on whenever I'm thinking about data driven decision making, I think this is more like-- I think one of the points you made around, like there is a small teams of people would have to make sense of a ton of data. And it's a very-- and it's a very complex and difficult problem.

[01:03:57.55] But one thing that I often think gets ignored when we consider transparency, because everyone's talking about transparency about the data, but what about transparency around what's missing from the data? Because this is like whenever I'm talking about-- I teach-- I used to teach a class on data and society.

[01:04:13.42] And one of the things that I went through was the data science model that people are using to make decisions and organizations, or do all this other work. But I often say like, where does the data come from? Who created that data? Under what assumptions was the data created? What is missing from that data?

[01:04:30.66] There's a lot of different ways in which you can think about transparency there. And who's being power or who's given power, privilege through that data? And then also the people that are doing the data-driven work, how are their values and shaping and meeting what they're seeing in that? And then that then impacts the people on the other end in a very severe and serious way.

[01:04:52.86] MARGOT KAMINSKI: Yeah, I'm completely forgetting the name of it. But it's like the data origins report, right? Or the like-- yeah, and this too is part of the conversation about transparency and algorithmic accountability of where do you put in place recording and reporting requirements that could, again create these facts, right? Or establish the internal records that then could be used externally.

[01:05:16.52] So Rachel my question to you listening to too Andrea, talk about how hard it is to receive specific requests versus the data dump request. Do you see this in the government context as well?

[01:05:30.26] RACHAEL JOHNSON: Well, I think it's very different from the-- obviously the government context is quite a bit different from the private sector context. And one thing that journalists will ask me or they have to think about before submitting a request is, does the government need to know what I'm going to do with this information?

[01:05:51.68] And the response is no. I mean, that's your information. You don't have to justify why you want that information. You should be able to get it. It's related to you as a taxpayer. You're paying moneys for the government to collect this information. I had one case a little bit off track-- a little bit.

[01:06:15.43] I had one case where a reporter was trying to get access to that tracer database. And he was told in order to get access to this database, it's going to cost thousands of dollars for the folks who are maintaining the database to get that information to them. And if you really think about that, that's like taxpayers' dollars. So it's like the journalist is paying for the information that he's eventually going to get access to.

[01:06:40.75] I mean it is a little bit different in the private obviously versus the government sector because this is work that the journalist is

doing in the public interest. So if it's a consumer looking at getting access to this data it could be for a very different reason.

[01:06:57.02] But the other thing with a journalist getting access to metadata that is data that has to be disclosed under CORA. That is a public record. So if a reporter is a data reporter, and they want to get that metadata information, they're going to know how to use it and manipulate it to make sense to the public.

[01:07:20.03] So if you get a data dump, they're like, that's fine. Just give me the data. It's OK, I'll figure it out. So it doesn't matter what category that they received information in.

[01:07:30.73] MARGOT KAMINSKI: Thank you. I'm sorry I hijacked the Q&A. So we have Daphne and I'm going to go five minutes late on this. So you all have warnings. So we can have more questions.

[01:07:40.51] AUDIENCE: Thank you. This is building on the points that Andrea made about the internal storage systems being messy and difficult. And so it's expensive to pull all of the data that makes up a user's profile. And I'm curious the kind of surveillance capitalism critique of platforms is, they have all this data.

[01:08:03.79] They can or are perfectly targeting us. They are using the data in the most rationalized scary way possible. And if that's not the case now, if right now they're storing it in a messy way where they could use it aggregate it but they're not into some beautiful profile of each of us, is there anything in the law that you guys work on or the practices you guys work on that would tell us like when do we want to keep it messy, or do we never want to keep it messy? Because of the transparency goals et cetera.

[01:08:41.74] ANDREA MACIEJEWSKI: Let me try and reiterate to make sure that I'm understanding correctly. Are you saying from the corporate perspective is there any incentive to keep messy databases?

[01:08:53.25] AUDIENCE: Sorry, I'm asking from the public policy perspective, do we want laws to drive those databases to become very clean so you really can do individual profiling on people much better?

[01:09:04.95] ANDREA MACIEJEWSKI: So I think it's-- I have an answer, but I'm not sure that it's going to answer exactly what you're asking. So I think personally and also from a corporate perspective, I do think that the laws should be pushing to have cleaner data. Like have your data in centralized areas, understand what you have, where you have it, and why you have it.

[01:09:27.36] I don't think that it's in anyone's interest, including the companies to have these databases in unknown places with unknown information. It poses a huge risk to the company to have a bunch of employees from 20 years ago, all of their HR records in an unknown

database that can be breached, and then all of a sudden you have a huge problem.

[01:09:47.02] I think that where the privacy laws are going from a data mapping perspective is probably the right direction. And I think from a public policy standpoint, maybe perhaps the concern is that having cleaner databases will create more advanced profiles, because you now know what you have, where it is et cetera.

[01:10:09.33] But in conjunction with creating data mapping its incentives, all of the laws are also creating incentives not to use large advertising. And frankly, a lot of the big platforms such as Google are starting to—

Panel: Transparency's Tradeoffs

<https://www.youtube.com/watch?v=xDHvCYvK4jw>

[00:00:01.53] MEG LETA JONES: Thanks, everyone, for staying with us for our last panel of the day. It will not disappoint. I am Meg Leta Jones. I am a graduate of CU Boulder, Atlas program in the Engineering School here.

[00:00:21.75] And when I was here, I also worked at Silicon Flatirons. So I'm very happy to be back. And I'm excited to have this crew with me to talk about technology transparency trade offs.

[00:00:37.62] Which of course, when you do the last panel, your thing has already come up a bunch. And so we've talked a little bit about this before. But we're going to focus on transparency trade offs. But I would also like us-- I think it would be beneficial to me and I bet a lot of other people, to also think about framing.

[00:00:58.11] Like how should we walk out of this room at the end of today and think about transparency. Tech and transparency. We also have one panelist who is Zoom in. Let me do introductions. And I'll start with you Hannah.

[00:01:17.58] Hannah Bloch-Wehba is an Associate Professor at Texas A&M School of Law. I think this is working magically. I'm very impressive. On the end, we have Eric Goldman, Professor and Associate Dean of Research at Santa Clara University School of Law.

[00:01:35.67] Next to him is Emily McReynolds, who works on AI Policy and Research at Meta. And then next to me is Chris Morten, Associate Clinical Professor of Law at Columbia School of Law. And Patty Limerick, who is a Professor of History here at the University of Colorado.

[00:01:58.51] So let's get into it. Our first question was teed up in the last panel. But if you weren't paying attention to the entire thing, a lot of things happened in the last panel. So Eric could you speak to one of

the questions that came up before, which is how we should think about free speech law as it prohibits transparency?

[00:02:26.22] Which to me and probably for a lot of people seems counter counterintuitive. What limits does the First Amendment place on transparency specifically, with regard to content moderation disclosures?

[00:02:41.97] ERIC GOLDMAN: Thank you. And I'm so delighted to be here. Thank you to Silicon Flatirons for organizing this event and putting together, and to my co-panelists, and to our moderator for doing such a great job. Let me just start just to make it clear. We're going to talk about trade offs on this panel.

[00:02:58.97] I'm guessing and certainly I am pro transparency, who isn't, right? We all want more information. Like thing that we all value is we want to know more. We feel we have greater agency and control when we know more. And I'm a researcher of course, I want more information.

[00:03:18.35] I can do more things if I know more about what's going on. But that's voluntary. When we give voluntary disclosures then that's between the company and the public. And that's fine. It's the mandatory transparency that starts to raise questions.

[00:03:36.38] And Amanda already covered the ground more beautifully than I could. So I'm going to just carve off a slice of the issue and really focus on a category of compelled transparency, that I call editorial transparency. This is trying to get into the editorial decisions and operations of companies.

[00:03:57.23] How are they structured? What are they doing? What decisions have they made? And what policies are they following?

[00:04:05.21] In my papers, I lay out a taxonomy of different types of ways that these regulations can be structured. One is that you can structure disclosures about a company's editorial policies. So this is saying, "Tell us in your terms of service, what things are OK and what aren't?" We can have another set of disclosures that are basically explanations, which have come up several times today.

[00:04:27.47] "Tell us why you made the decision that you did?" Now, this could come up with a privacy context where you say, "Explain to us how your algorithms work." But in this context, I'm thinking about, "Explain to us why you chose to publish something or why you chose not to?"

[00:04:41.27] Why you chose to put it above something else? Tell us why you gave this many words to the story and why you chose to feature it or not?" A third category is statistics, tell us what percentage of things you did?

[00:05:01.07] We talked about it earlier about this prevalence rate. What percentage of the items do you actually catch or how many times have you removed an item for a particular reason? And there's a fourth issue. And this is the one that I find a little frustrating when I talk about transparency because often I find people don't think about it or get to it.

[00:05:18.23] It's why I call the source data disclosure. In order to actually evaluate the accuracy of any of the disclosures that we've just discussed, we need more information from the company to see what they saw. So for example, if they chose to unpublished or never publish things in order to then calculate the statistics, we need to see that unpublished material.

[00:05:40.40] Or if they're applying their editorial policies probably, we need to see what they actually did screen out in addition to what they didn't. And I can't remember who said earlier today, actually each of those raises its own constitutional questions.

[00:05:59.30] We actually have to analyze them differently just like we would any other kind of transparency. One size doesn't fit all. We have to say, "What is this law requiring? What does it do?" I'm a skeptic of all of them from a legal standpoint because of really two things that I think Daphne really highlighted earlier today.

[00:06:16.89] First, the fact that in order to do the enforcement, the government's going to be rooting around in this source data saying, "Tell me what you saw and let me come in second guess those decisions." Now, we might not care if we're talking about sugar content in a can of corn, but we care a lot when the government is come in saying, "Why did you publish this?"

[00:06:36.08] What was your rationale? How did that fit your rules? Did you probably disclose in your statistics? And I'm going to second guess all of that?" And so that enforcement issue I think becomes very problematic because it basically puts the government in the role of the editor's shoes saying, "I'm going to question what you did and why you did it."

[00:06:55.13] It also should be acknowledged as again, Daphne pointed out that many of those enforcement will not be done because they're trying to get to the truth. It's going to be done for partisan reasons because publication is a power center and governments want to control that power center. So the reason why they're bringing in enforcement is because they think there was a falsity.

[00:07:17.12] They want to try to exercise their power in order to advance a usually partisan agenda. So this interaction between the editorial function and the government coming in second guess it creates, I think, a whole range of constitutional friction. And if you ever find transparency being compelled, ask the question, how is it going to be enforced?

[00:07:42.53] Who's going to enforce it? What are their motivations and what are the consequences when that is weaponized for a purpose that you don't support? The other concern is knowing that there's this hammer of enforcement hanging over the heads of the publishers. They change their decision in advance.

[00:07:59.57] They look for the lowest friction decisions that will avoid the risk of a future enforcement for partisan agendas. So that means basically they're preguessing what the enforcers want and then providing that. Not what's in the best interest of their audience, but in the best interest of keeping the enforcement angles low.

[00:08:18.89] And I'm sorry I can't recall who was sitting here earlier talking about the cost of dealing with those enforcement, the requests. But that actually is in spades when it comes to these publication decisions. The government coming in and saying, "We don't like what you're doing. We're going to use the powers of our enforcement tools to change your behavior."

[00:08:40.38] So these are the reasons why I have skepticism from a constitutional standpoint about all of the different types of transparency that could be compelled from editorial operations or decisions because of the fact that in each of those cases, they're changing the publication decisions in a way that distorts the freedom of speech and press.

[00:09:08.10] MEG LETA JONES: Thank you, Eric for putting that landscape in place for us. I feel like all of our participants can build off of different areas. I just want to follow up really quick on the last thing you were talking about in terms of bipartisan weaponization.

[00:09:22.47] Is what you're just saying true for all mandatory disclosures? And you're like, "Let's not do more of those." Meaning that all mandatory disclosures are being weaponized for partisan reasons. And we don't want to add to that plate or that there's something special about this particular weaponization of mandatory disclosures that you're not interested in?

[00:09:51.33] ERIC GOLDMAN: Yeah, and I do think that that's the question that you should be asking with every type of mandatory disclosure. Again, who's the adversarial threat in this equation and what are they going to do to advance their agenda?

[00:10:04.27] But I really think there's something unique or special about editorial disclosures. About trying to get into the newsroom or the Heads of Editors and say, "What are you doing and why are you doing it?" Getting into their heads is a qualitatively different thing than get into the heads of a manufacturer of ordinary goods and services.

[00:10:22.98] Where if they change their decision, it doesn't have speech implications. The way that if a publisher changes their decisions it unavoidably has speech implications.

[00:10:31.83] MEG LETA JONES: Great. Thank you. Editorial decision making, inside people's brains, one version of transparency trade off. I want to ask you about automated decision making also known as Algorithmic Accountability.

[00:10:50.18] Can you talk to us about the trade offs, maybe inherent or just the ones we're looking at with Algorithmic Accountability. And what limits there should be given that often the algorithmic decisions are made using highly personal data and producing highly personal inferences.

[00:11:12.30] HANNAH BLOCH-WEHBA: Yeah. So first of all, I want to say thank you for having me. I'm so sad that I'm not there in person. But I guess my disembodied head on a screen is almost as good. And Thank you, Meg for moderating.

[00:11:27.15] So I want to build a little bit in the second half of what I'm talking about on what Eric was just saying. But to start, I want to situate the debate about algorithmic transparency within a broader debate about accountability. So I'm really thinking about the use of algorithmic decision making in public sector settings, right?

[00:11:51.64] So what happens when the government uses some algorithmic tool to make decisions that have dramatic implications for people's rights and their livelihoods? And so in this setting, we're really talking about accountability for government actors as well as accountability for technology. We're thinking about technology as it interfaces with government programs.

[00:12:22.17] And so I find it helpful and necessary to articulate a little bit what the potential overlap and maybe differences between algorithmic transparency and government transparency might be. Because to some extent when we're talking about transparency in this setting, we're talking about a necessary precondition for accountability. Both of the technology or of the people who made the technology and of the government itself.

[00:12:53.04] And that's the basic presumption of government transparency law is that you can't hold to account what you don't know about. And you need transparency as a precondition for accountability. But the usefulness of transparency and of different forms of transparency enhancing intervention depends then on the thing that you're trying to learn.

[00:13:18.10] So when we're talking about government transparency, transparency is a crucial component of self governance and democracy. It's at the core of press freedom and free speech. But when we're talking about algorithmic transparency, it's not always self evident what kinds of values we're seeking to serve.

[00:13:40.15] We have a shorthand understanding in the government transparency context of what those values are. We could just call them

democracy values. But in the algorithmic transparency context it's not always so obvious. You might think that given the increasing democratic salience of technology, there are also democratic values at stake here particularly in the public sector context.

[00:14:05.61] But a lot of the time there are also concerns that transparency might serve counter democratic values. For example, by allowing bad actors to game the system or to effectively steal individual data. So it's not always obvious that transparency as such is necessarily a good thing.

[00:14:30.85] I'll come back to this in a couple of minutes because I think the answer to whether transparency works depends on how it's designed. So one helpful way to think about algorithmic transparency, I draw from the work of Jenna Burrell, who has distinguished between three different kinds of algorithmic opacity.

[00:14:56.70] There's opacity as secrecy. Algorithmic opacity as intentional concealment of some kind of decision making mechanism. There's opacity as lack of knowledge. Which is we might all know that an algorithmic decision is happening but we might actually lack the ability to understand how it's working in practice.

[00:15:19.90] And then there's opacity as incomprehensibility. Technological opacity that's caused by the way that an algorithmic decision making mechanism is designed. And this is I think most obvious in the context of AI and machine learning.

[00:15:38.29] So when we think about those three different kinds of opacity, it becomes clear that we can't just slap a uniform transparency mechanism on to solve all three of those problems. That existing transparency as disclosure regimes might effectively combat intentional concealment, but they don't help us get the information that we need to comprehend how an algorithm actually works in practice.

[00:16:10.54] And so if we wanted to design an effective algorithmic transparency regime to promote accountability, then we have to get at a richer menu of problems. So I want to come back then to the second part of your question, which is about what are the limits to transparency.

[00:16:33.21] I think as lawyers, we often have a very particular vision of transparency as disclosure to the public. And that's in part informed by our legal system. The right to laws like the ones we were hearing about on the last panel. Or by, for example, rights to notice.

[00:16:53.97] The right to know that something is happening whether it's general or whether it's about me specifically. But one thing that we learn from distinguishing between government transparency and algorithmic transparency, is that there might be a richer menu of

options to enhance transparency than just compelling public disclosure.

[00:17:16.54] And so in some of my work I've tried to distinguish between transparency of what to whom and at what time. So for algorithmic decision making, we might start by asking, what are we trying to enhance transparency of? The fact that a system exists.

[00:17:32.43] That it's being used. That a decision is happening. That it's happening to you particularly. And who should know that this is happening? Whatever what is, who should know about it?

[00:17:45.10] Is it the person who's affected? Is it regulators? Is it courts? Is it the general public? And then there's the question of timing.

[00:17:53.97] When should we know? Should that happen before a decision is made? Should it happen after? Should it happen repeatedly, continuously?

[00:18:02.34] And so I think dis-aggregating these kinds of questions helps us to think about could we imagine an algorithmic transparency regime that is more sensitive to privacy because it doesn't entail public disclosure of the kind that we've been conditioned to think of as the gold standard. So we've been trained to think about disclosure as the paradigm of transparency.

[00:18:31.89] But I think there now in these novel and emerging algorithmic transparency efforts a much more nuanced set of tools. So I'm thinking about impact assessments, which tell us how automated decisions have certain effects on society audits. Which tell us more about how the technology is actually working and researcher access to certain kinds of automated decisions without public disclosure.

[00:19:02.62] So I think it's possible in short to imagine transparency enhancing regimes with a much more limited role for public disclosure and a much heightened role for other forms of knowledge to emerge.

[00:19:21.96] MEG LETA JONES: Thank you so much for organizing that so neatly. One of the things that you said related-- got me thinking about the question that I asked Eric. And I'm going to use it as my transition here to Chris which I'm thinking about whether incomprehensible opacity is particularly vulnerable to weaponization and the trade off is a significant loss in legitimacy.

[00:19:54.42] And so Chris, when we think about trade offs with regard to scientific information, technical or medical knowledge transparency of those types of information, how should we account for these many actors in the current state of affairs. So given that increasing ease of identification, how should we consider public disclosures specifically scientific and medical information.

[00:20:25.85] And related to Hannah's last remarks, what privacy related limits should we have in those contexts?

[00:20:33.46] CHRISTOPHER MORTEN: Yeah. Thanks so much, Meg. Thanks so much, everyone. It's really a pleasure to be here. And as I think Meg's question previews-- I'm a little bit of an interloper in this group. So I'm not a data privacy lawyer.

[00:20:48.08] I'm not someone who works on content moderation. I'm really a health lawyer. And in that capacity, have worked on the governance of scientific and medical data, including sensitive personal medical information and including information that is trade secret or is alleged to be trade secret information. So I bring a little bit of knowledge of how that knowledge is governed.

[00:21:17.09] So I'll say, I agree with the premise of the panel to a point that there are trade offs to transparency. But Meg you asked I think a little bit about framing. And I will simultaneously I think challenge or problematize the frame because I don't think there's a simple trade off here.

[00:21:35.36] I think it is possible to unlock benefits that are greater than the downsides. Or the trade offs are not linear. And this goes actually to something that Hannah just said, that when we think about transparency I think some of us as lawyers, I at least as a lawyer for a long time thought about transparency as meaning public disclosure.

[00:21:53.33] And that comes from the Freedom of Information Act. It comes from a lot of open government laws. It comes from a lot of places in the law. But we tend to think of transparency as on off binary choice.

[00:22:04.22] But to quote Hannah, again, I think we actually have a much richer menu of options than the history of data sharing in science and medicine shows that. And that means that we can unlock some of the benefits of data sharing without exposing individuals to great harm and without exposing companies that share information to great harm.

[00:22:26.00] So that's the main thrust of my remarks. So I'll say in connection with that, I'm optimistic and supportive of legislation and regulation that would mandate more transparency from tech companies today. And I feel particularly having listened to the panels earlier today, it seems clear to me than ever that the tech industry is too secretive.

[00:22:46.52] And we the public should develop responses to that. So let me get a little more concrete about the medical and scientific data sharing that I'm referring to. And I will plug shamelessly a paper that I'm working on with Salome Vilgjoen at Michigan and Gabe Nicholas at the Center for Democracy and Technology.

[00:23:06.23] So we actually have something in the works about lessons from medical and scientific data sharing that we think are transposable or applicable to social media platforms and other tech companies. So in science and medicine today, we have after much contestation a much experimentation, legal and institutional and technical frameworks that permit sharing of intensely sensitive data. So this includes clinical trial data,

[00:23:31.07] Includes individual patients medical records, genetic data commercially valuable data on how companies conduct their R&D and much more. And we have public and private bodies that steward and share this data with third party researchers. I should say actually most of the focus of what I'm talking about here is researcher access.

[00:23:48.71] And I understand that there are many other important facets to transparency. And researcher access is the facet that I know best. So quickly I'm glad to talk more about this folks. For instance, we have for example, working data sharing programs at the NIH, National Institutes of Health Administrators, Food and Drug Administration, Canada's Health Regulator goes even farther than FDA does.

[00:24:10.37] We have private data sharing initiatives at universities like Harvard and Yale that take sensitive medical data and make it accessible to researchers. And we have no federal law that mandates the drug companies, device companies. Other companies with very strong incentives to secrecy that resisted data sharing for decades are now obligated to share data some with the public at large without condition, without restriction.

[00:24:36.40] And some in these more selective and conditional ways that Hannah gestured at. So I'll say again, yeah, I think the choice between secrecy and transparency is not on off or binary. We have in medical and scientific data sharing all tools, legal tools technical tools to constrain who gets access. Limit who gets access. Limit what uses they make of data.

[00:25:02.44] And a couple of the important ones. Glad to talk more about this. Data use agreements are now ubiquitous. We have technical constraints that prevent users of data researchers from downloading complete data sets. We have differential privacy in some limited contexts.

[00:25:15.52] All of these in various ways shape the uses that are made. I also think it's really interesting the law and the specific data use agreements that are imposed on researchers often impose positive commitments on the users of data. So they're obliged for example, to report safety problems to regulators.

[00:25:30.82] I think all of this is really interesting and perhaps some of this could be applicable. By the way, Meg you mentioned I think specifically the risk of re-identification. And I will say that's something a concern on my mind.

[00:25:43.36] I think a really vivid important concern when you're dealing with individual patients medical histories. A lot of people whose data is implicated here are some of the most vulnerable already. And the tools that medical researchers and the data sharing stewards have come up with keep the risk of re-identification at the center.

[00:26:02.87] So I think I'll stop there. I'll just reiterate the point that I started with that I don't think the trade offs are linear here. I think more access or more transparency at least in terms of research or access does not necessarily mean proportionately more harm or more risk. I say that again with some humility that's the world I know, and I realize there are a lot of differences when we get to platforms.

[00:26:25.07] MEG LETA JONES: Well, Chris that sounds great. Should we just do that? I mean, I feel like you just pitched us. Are there-- tell me one downside to this.

[00:26:32.44] Tell me one thing that doesn't work well in this system.

[00:26:35.37] CHRISTOPHER MORTEN: Also there are huge problems.

[00:26:39.13] PATTY LIMERIC: Disclosure.

[00:26:39.70] CHRISTOPHER MORTEN: Yeah. So I'll echo-- I mean, some of the really, really important problems that others have said. So I think medical data sharing today is working much better. Like pharma and biotech companies today have to share certain kinds of data. Do they comply 100%? No, they do not.

[00:26:55.61] And I as a lawyer, I've litigated it. I've litigated. I've done advocacy.

[00:26:59.90] I've done other work to try, for example, to increase compliance by drug and medical device companies with a federal law that requires them to report the results of clinical trials and report their methodology when they run clinical trials. Compliance with that law today is about 75%. So not perfect.

[00:27:21.53] And there are problems with enforcement et cetera. I step back, though and I say 75% compliance is pretty good. There are things that we can do with 75% compliance that we couldn't do with 0% compliance. And the world of data sharing today is far better than it was 20 years ago when we relied on voluntary commitments from these same companies when they would cherry pick which data to share et cetera.

[00:27:46.94] So but that is. So the problem of lack of compliance, the problem of lack of resources in the public governors of this data. So NIH and FDA, huge problem. Problems of capture and institutional inertia. All problems.

[00:27:59.20] MEG LETA JONES: OK, OK. I thought maybe there was something to this. But thinking about mandatory disclosures of data is a great-- I think question to pose or a great subject to pose to Emily, who works at Meta.

[00:28:17.06] Emily, tech companies are approached for a ton of data all the time. And transparency regimes can expose lots of user data that makes them-- that makes you really, really vulnerable. When companies like Meta see regulatory calls for increased transparency, how do they and how should they think about them?

[00:28:44.61] EMILY McReynolds: Thanks Meg. And thanks for the invitation to be here. I wanted a little bit situate my expertise and what I do but in answering this question. So I'm on the AI Policy team at Meta.

[00:28:56.28] And what that means is sitting in the privacy. And data policy team we think a lot about the implications for data and how that comes up in machine learning and AI. And where we sit, I think highlights the importance of thinking about what we do with data in terms of transparency.

[00:29:17.32] So the AI Policy team works across the company on issues like AI transparency. We act as the internal subject matter experts. So looking at provisions, the proliferation that we're seeing of important potential regulation from the UAI Act to Algorithmic Accountability Act here in the US.

[00:29:37.77] Usually, I have a slide that's a big picture of the world. And so many bullet points of all the things we're looking at. We have transparency efforts in Asia, in Latin America, looking at all the different laws that are coming and how we can respond to those. I think it's really important to be responsive to these proposals and how they might be implicated.

[00:30:00.63] But I'm coming at it from a research perspective. So I've spent a number of years looking at how we do documentation? How do we do impact assessments? How do we think about those things in an effective manner?

[00:30:15.82] So when I work with our research teams or with our internal product teams, I often bring in external expertise. I come to events like this and I learn new things about approaches from health care data experts. And thinking about it in terms of building these standards in a cross disciplinary, cross industry, cross regulatory way, I think that's obvious for an international company.

[00:30:43.23] But the influence that research plays in that space it might be less obvious. One of the things we have is an approach through five pillars of responsible AI. And so when you're building AI responsibly after a proliferation also principles-- I think we're over 85 principles sets of principles on how to do AI ethics and deal with these kinds of issues.

[00:31:08.95] And so one of those is transparency. And I'll call back to Hannah here. When we're talking about transparency and when we're talking about explainability, which are sometimes used interchangeably. It's really of what to whom and when. So when we look at the different options that regulators are exploring, that companies are considering complying with, what does it look like?

[00:31:35.94] Is the trade off-- the trade off in my opinion shouldn't be between sharing data or not sharing data. But sometimes the data isn't the most helpful thing. What you want to understand isn't maybe 1,000 models that have built a system based on millions of points of data. You might want to understand why this system exists. So over the last year, the Meta launched this year the AI system card.

[00:32:03.66] So there's about a five year history now looking at how you look at data, how you provide transparency around data, how you provide transparency around machine learning. So everything from a data nutrition label to a model card to data statements when working in natural language processing. I'm citing a lot of academic work.

[00:32:23.76] And if I listed all the names, we would be here 10 minutes from now. So just know huge amount of respect to the researchers that are still working on this today. I think what we've come to is in explaining what to whom and when really thinking about levels of explainability. And so the company and particularly the responsible AI teams that I work with, have thought about who needs what explanation when.

[00:32:50.13] And how much data might be required for that? How much information about the machine learning model might be required for that? One of the things I'm really proud of is some of the academic publications we've done around this topic. Really exciting titles like prescriptive and descriptive approaches to machine learning transparency.

[00:33:11.10] But what that says in a user facing, in a public facing way is that we're trying to provide the transparency that is being asked for. And there are trade offs in how to approach it. But to directly answer the question, I think companies should and need to be responsive to regulation that's being considered and be a part of these conversations.

[00:33:34.83] MEG LETA JONES: Great Thank you so much, Emily. I think that is one of two narratives around transparency that Margot and I had been talking about as we were speaking with Patty before the conference. So Patty is really an expert on narratives in her own career.

[00:33:57.57] And let me tee this up properly. So we were talking about how transparency is in this position where there's two teams. One are like, "Yeah transparency is vital. It's obviously important for accountability." Versus the, "It's really corrupt and it's just not worth

much. And we should be spending our time on other things to try to do governance."

[00:34:21.21] As an expert in narratives and counter narratives and maybe an expert on that topic is not right. But I think you have embraced this as part of your career, as an author of really one of the most notable texts on the History of the American West. I would love for you to talk about how you came to maneuver within a narrative that you had challenged, and why you did that?

[00:34:45.81] And how we might think about moving forward within or around an idea of transparency?

[00:34:54.21] PATTY LIMERIC: I think I can do that.

[00:34:55.22]

[00:34:55.26] MEG LETA JONES: All right.

[00:34:55.73]

[00:34:55.79] PATTY LIMERIC: We'll find out. So Western American History. Oh, my goodness more than 35 years ago it was really stuck in a shall we be celebrating the westward movement of white men or should we look at the whole complexity of the population?

[00:35:14.26] And it looked like we were going to be locked there for a really long time. And it was so boring. We had argued that just into a corner that debate just wanted to go away and die or rest I guess. So but we just kept at it. So we were doing this shall we be honest and accurate in our version of Western history and a debunk it?

[00:35:33.22] Or shall we hold to some forms of identity that are crucial to some people? I mean, these have some relevance in American society today. But anyway, so that was where I was on the debunking side. And I was fierce. And I was persistent.

[00:35:45.91] And several years passed with me just debunking away with everything I had and then suddenly thinking, "I'm not getting anywhere." I'm having no impact. And the people who already agreed with me, oh, they were really, really agreeing but they already did.

[00:35:59.71] So this is not satisfying. And maybe it had some minor satisfaction of self-indulgence but not sufficient. So I just felt that I certainly wasn't gaining ground. And I went to speak in Durango at Fort Lewis College once. And I had the New York Times--

[00:36:19.32] This is quite a few years ago. Had an inside the front page ad for a book about the American West a novel called The heart of the West. And it was very overstated and clearly a nonsensical book.

[00:36:31.44] And I held it up-- I held that ad up to the students. And I held my book, *Legacy of Conquest* and I said, "OK, students in Durango here vote. How many points would you give to the influence of my book, *Legacy of Conquest* and how many points-- scale of 100 would you give to this *Heart of the West*?"

[00:36:48.30] And it ended with something like, "Montana, was not the only frontier for the schoolmarm who was facing it." It was such a ridiculous name. So I was very clear how they should vote. No, obviously.

[00:37:01.83] These very honest students, honest to have followed in Durango. They voted-- they gave the colorful *Heart of the West* book 99 points. And they gave my book one for influence and impact. Well, shall we weep? No, we won't weep.

[00:37:16.95] But we'll say that there's a lesson there I finally just thought, "This can't go on like. This is getting ridiculous." So that's what I did what-- Meg is talking about here I just thought, "OK, tried that. Did that. Debunking two opposing points of view, I'm going to line up with one.

[00:37:30.93] I'm going to put everything I have into it." And then I thought, "This isn't really going." So what I did, I didn't do it today I'm sorry I bought Western wear. I didn't buy it but I didn't wear it today either. So I started wearing cowboy boots.

[00:37:42.48] I started-- I have two Stetson's. I started just thinking, "It's not if you can't beat them, join them." It wasn't that. If you can't beat them co-opt and confuse them. So that would-- I think that's the first time I've used that particular slogan.

[00:37:57.95] But I could use it on a t-shirt or maybe you could use it on a t-shirt because I think everybody has said some version of stark choices. Might work in some zones. And certainly compulsive mandatory. We're going to pin you and you're going to be nervous and shut up. Because you've been pinned up.

[00:38:14.18] That's very persuasive. But mostly I think people were saying some version of this is different in different situations and either or constructions. I mean, you did use the word binary. That's not really working.

[00:38:27.36] And it's just much more stimulating and fun to be inside what you once saw as a very divided battleground. It was just more fun to stand in the middle and say, "Well, if you were planning to have someone in the middle to scorn-- Oh, here I am. But maybe we could have a discussion maybe I could be the moderator or something."

[00:38:53.18] So that's what I think was the dream here is that I might be able to say something that would be like, "Well, there's other ways to do it. To say trade offs still suggests that there's something or I shall

trade you this for that. And I'm getting the sense that maybe he's not that clear here."

[00:39:09.39] So what I would like to tell you about is a wonderful project at the South American West. The former that now descendants of the American West. So it's not the American West starting again. So what used to be is the American West now still has launched a project on interpreters and translators in Western American history.

[00:39:26.76] They at any treaty negotiation between Indians and whites the most important person there is the interpreter. Nobody writes. We write about the generals. We write about the Chiefs but people labeled Chiefs.

[00:39:36.62] And the interpreter is in the middle and carrying the weight of the whole event. And if that interpreter performs well, fewer people will get killed. If the interpreter screws it up, then expect mortality to go on that. So I didn't have that in my initial notes here but I just thought maybe that's what would be helpful from the Western American history.

[00:39:53.69] Seen here is that empowering and the 21st century are the example of these poor souls. Most of them not prospering leading citizens who stood in the middle and said, "I think what they're saying over here is this. And I think what you're saying because it's possible to do full disclosure and still leave everyone deeply confused.

[00:40:16.56] And depending on what form of data collection and transmission you have, the more complicated the calculations the more likely you can disclose. And no one will know that you did." So that can't be what transparency means.

[00:40:34.29] I want to just quickly say that I think paradox is the magic word. I spent too much time thinking of contradiction. Thinking of even hypocrisy or inconsistency. And then it just seemed like paradox by which two things seem unrelated but actually are very related that, that is true not only for the process of deciding transparency and disclosure.

[00:40:58.15] But also for what you do when something gets transparently disclosed. So that would be-- and then I would just say that one of the great things that's going on in the field of Western American history could have been disclosed any time over the last 150 years. But no one did that because only one historian and his proteges asked the question.

[00:41:17.70] So I want to conclude with that, that every teacher in every high school American history class has a unit on "manifest destiny." Anybody here take that? Yeah. So Drew Eisenberg University of Kansas is writing a book which should be out soon. He has a couple of proteges.

[00:41:34.50] And it turns out that term was hardly used in the last half of the 19th century. John O'Sullivan, a hack journalist, coined it. He was proud. Nothing much happened.

[00:41:45.06] Then historians in the early 20th century trying to write a history of the United States that would be unified and wouldn't just collapse under the weight of the Civil War. They went back and dug up that term "manifest destiny" and started using it all the time.

[00:41:58.95] So no people-- most westward settlers, did not think of themselves. There's no evidence how can we prove or disprove no evidence that they thought that they were creatures of a divine mission occupying the West on this mission. They wanted land.

[00:42:13.52] And if it turned out that the Pacific Coast became the Pacific Coast Republic. And they got the land they wanted. And it was modeled on the United States but they were OK with that. So when you think of all the nonsense given in high school history classes by well-intentioned people, the American people believed in manifest destiny.

[00:42:30.50] No, a hack journalist coined the phrase and then it got revived and revitalized. So I'm ending with that because it probably seems to have nothing to do with anything. But also because I think it's key to what is it that human beings are saying to each other.

[00:42:45.93] And when do they accurately assess what they're saying to each other? And when do they just go down a path that's entirely different? And so I'm thinking that is at the core of the question of what is functioning is transparency. And what is a failure of that and what is it irritation and imposition with that?

[00:43:03.29] I hope that made some unit of sense. And I can talk to people privately afterwards if you were saying, "What that have to do with anything." But keep an eye out for that book Andrew Eisenberg on reconsideration of manifest destiny. So.

[00:43:18.60] MEG LETA JONES: I will keep an eye out for that. I am intrigued by this middle position that I think both Chris and Hannah and actually Emily too position this. Which is like we're not into these binaries. We're not into this trade off language.

[00:43:38.27] We've got these other tools that will help position us more strategically to choose Patty's words in the middle. And I'm going to pose this question to Eric while hopefully you all are readying your questions because I'd like to just hash out as many questions here at the end as we possibly can. But Eric, does the middle have firmer constitutional grounding than other forms of transparency?

[00:44:03.80] So these impact assessments, audits research access all different angles into mandatory disclosures or maybe they're not. Should we think of those as mandatory disclosures? How should we

think about them in the constitutional moment that you set up for us at the beginning?

[00:44:25.53] ERIC GOLDMAN: So there are a lot of things that could be in that middle ground. And I'll talk about the three you mentioned. But just to be clear, if we're talking about trying to understand editorial processes, I reject the premise of that question at its core. So it was like, well, what if we do it less sensorially?

[00:44:44.03] I'm like you lost me there. You know what I'm saying? If the goal is to control how content publication decisions are made, then I think we have the wrong goal. And we need to reject the goal on its premise. So you say something like impact assessments.

[00:44:59.51] And I don't really see the role of that. And when it comes to something like content moderation at least from a transparency angle. That's really the whole point of impact assessments when you think about from an editorial standpoint say think before you publish. Which sounds pretty bad.

[00:45:14.27] Actually the kind of thing that we probably would not support. The audits, I do talk about audits in my paper. Audits basically just deputize a proxy for the government to come in and ask the questions that the government is asking directly. And the problem with audits at least for my purposes of the taxonomy that I laid out for you is that if we question the auditors integrity, you're going to have to get all the data that was supposed to be not available to the government.

[00:45:46.19] Anyway, it just becomes a proxy for they gather the data, they review it and then if we question what they're doing, we've got to look at it again all together. So if you trust the editors and you're willing not to second guess them perhaps that's fine. But I don't think anyone does that see maybe Arthur Andersen.

[00:46:05.36] And then researcher access- and can I talk about this in my paper about scraping is one example. Scraping I think does solve some problems. It raises a bunch of other problems. And so I think that's a great example of a true trade off.

[00:46:21.56] What do we get from scraping and what are we going to give up? And the thing that we didn't talk about there's some competitive gaming from scraping that I think needs to be considered. But it's like there's simply like a volume issue. You know, how many different researchers are all sending their scrapers out and how much does that impact the functioning of a website?

[00:46:40.10] They're not there to be scraped. They're there to actually serve their clients. And so the scraping becomes like a tax or a burden on top of the actual functioning of the operations. The other form and we talked about this I believe in the first panel was that companies can provide data sets.

[00:46:58.14] But if they're predigesting the data sets then that doesn't solve the problem because they're laying the foundation for the researchers to find only what they want to find. And if we don't believe that if we want to question whether they're predigesting the data sets, well then we're right back to the same problem. Which is the government has to come in and say we don't think you disclosed everything.

[00:47:19.88] And now we haven't really solved the problem anyway. So I think that the transparency itself is supposed to be the middle ground between outright censorship and between market forces. Let's say fair.

[00:47:35.66] And so on terms like disclose, we can watch and if we don't like what we're doing, then we can let the market decide or we can come in and intervene based on that disclosure. I think the middle ground of transparency actually starts to get that muddled. So I actually prefer looking for alternatives to binaries as well.

[00:47:54.75] But here, I actually think that anything that we're going to do that's an alternative to, yes, the government can mandated or no the government can. I think we're going to find is probably actually either not solving the problem or it's actually just as bad.

[00:48:12.62] MEG LETA JONES: Chris, Hannah would either of you like to respond to that while I drum up a student question. I don't really I can't quite tell who's student. So I might need Margo's help.

[00:48:25.77] CHRISTOPHER MORTEN: Hannah, do you want jump in? I can venture something.

[00:48:31.11] HANNAH BLOCH-WEHBA: Do you want to go first Chris while I formulate my thoughts?

[00:48:34.14] CHRISTOPHER MORTEN: So I will just say not only am I not a data privacy lawyer, I'm also not a constitutional lawyer and definitely not a First Amendment lawyer. And so I know a little bit about Eric's work but cannot speak convincingly on the potential susceptibility of I guess a wider ranging transparency mandate to a First Amendment challenge.

[00:49:04.65] I will say-- what can I say. I feel I know just enough to be dangerous about the intersection of First Amendment law with again, the space that I'm most comfortable with, which is pharma and biotech. And there to I cannot name the case.

[00:49:19.71] But I know that there are cases where drug companies or pharmacies or other holders of valuable data have been obliged to share with regulators certain information in their possession. And I think those were subject to compelled speech challenges. And I think that those survived to some extent which is to say some kinds of transparency forcing regulations.

[00:49:46.09] I think have endured in that space. I think they've been cut back. And Eric--

[00:49:52.51] ERIC GOLDMAN: I'm sorry. Do you mind if I--

[00:49:52.99] CHRISTOPHER MORTEN: Please.

[00:49:53.59] ERIC GOLDMAN: Just want to make sure everyone understands. I mean, this is a very common conversation that we have when we talk about compelled speech. Let's look at all the places where it is permissible. Now, why by analogy would this be different when it comes to the publishers being forced to disclose.

[00:50:07.51] I just want to be clear the threat models when it comes to publisher, transparency are very different than drug transparency. Things like in drug transparency worried about things like competitor gaming. Well, that's actually not an issue with publisher transparency. Usually the publishers aren't the ones trying to game each other.

[00:50:26.59] Instead we're worried about things like government state actors who are looking for ways to game the system. Or we're looking at things like the trolls or the spammers who are looking to game system. What we're looking at just the flat out censorship, how can a government act or shut down a line of conversation at once?

[00:50:44.32] And you just don't have that with the drug issues. It's just qualitatively different. That's not to say we can't learn something. I got to say I already learned some stuff from your talk. It was really great.

[00:50:53.53] But I think it's qualitatively different than the concern I have.

[00:50:57.39] STUDENT: [INAUDIBLE] student question.

[00:51:00.03] [INTERPOSING VOICES]

[00:51:03.51] MEG LETA JONES: Yes, go ahead and somebody give that student a mic.

[00:51:07.81] HANNAH BLOCH-WEHBA: So I think the hard question that is raised by this distinction right like maybe it's easy to say that certain kinds of regulation are unconstitutional with respect to publishers. But potentially constitutional with respect to the pharma industry.

[00:51:26.32] Doesn't mean that the pharma industry isn't going to use the First Amendment to try to align its position itself to be more like the publisher than a producer of widgets. So the first-- I think hard question is to what extent are the First Amendment arguments going to be categorically limited to a certain industry or business model?

[00:51:54.74] And I think that it's really hard to anticipate how they might be leveraged in other contexts with respect to the question of impact assessments or audits. I think that the arguments. The first Amendment is probably going to be bandied about as an argument against these interventions both for social media companies but also outside of that context.

[00:52:21.76] So when I think about regulating automated decision making in for example, the employment space. So New York just enacted a new law that prohibits employers from using certain automated mechanisms to screen employees unless they adopt certain safeguards including audits.

[00:52:46.21] Could we first see a potential first Amendment challenge to that kind of law? Could an employer or the maker of an employment algorithm make the argument that forcing us to open this code to scrutiny is itself a form of compelled speech? Of course, they could.

[00:53:05.95] And they probably will. Because we've seen this argument in many, many contexts because it builds in part on the notion that informational exchange is of necessity always speech. And to the extent that courts accept that baseline, then all like many different kinds of commercial conduct that rely on data, are going to be speechified.

[00:53:34.96] And thus regulation of those kinds of conduct are going to become vulnerable to First Amendment challenge. So that's not a comment on are the First Amendment challenges meritorious or not. But rather I think we need to think about these kinds of interventions through a First Amendment lens because inevitably this does appear to be the direction that courts are taking.

[00:53:59.72] And so I think that speech like challenges to what we might have previously thought of as ordinary regulations of conduct are becoming more and more frequent.

[00:54:13.00] PATTY LIMERIC: Could I just-- yeah, I'd like just to say that I think historians are so chronically driven mad with frustration because the people of the past, which most of them are dead and they just won't disclose. And it's very irritating.

[00:54:29.37] And they're just an annoying group of people really. And so I think like James K Polk declaring war in the Mexican-American War. And saying that American blood had been shed in a Mexican cornfield. No, not exactly.

[00:54:45.37] And so all the time we spent trying to think what we know Polk was squirrely in declaring that war-- we know that but we can't get inside-- actually we want to get inside his mind for heaven's sake. But it just seems like we are forever vexed and frustrated.

[00:54:58.69] And so our expectations are really modest for disclosure. And maybe that makes us a happier people because we have nothing that approaches-- that goes anywhere near our high expectations for what we will get from information about our fellow human beings. We're just always in a state of dismay over the fact that they're hiding from us.

[00:55:22.00] Because they die, which is very frustrating to have them just shut up from that. So I just think that we might be some kind of useful model that we have had. You may not think this, but we actually have made our peace with the fact that disclosure is always partial and no senses of that. And our expectations are very modest because they've had to be.

[00:55:41.80] And maybe that makes us happier people. I don't know. But I think the word-- I think Eric you were using the word accountability is something that can figure-- was it Hannah? OK, so the word accountability we would like to do that.

[00:55:52.12] We would like to say James K Polk was entirely responsible for the invasion of Mexico. And we'd like to hold him accountable. We'd especially like to hold Richard Nixon accountable. That would be a great joy, but he's squirrely too.

[00:56:04.93] And so we get more squirrely than we get full disclosure. And maybe you want to join us in having more modest hopes.

[00:56:13.77] MEG LETA JONES: Yeah that's-- I mean, this question of whether transparency makes anybody happy, I think is a good question. And whether more information makes people happy? And you're absolutely right.

[00:56:27.99] Historians have a relationship, a methodological relationship with the records that they have available. And I think whatever new regime hopefully, a new regime comes in this space, we will have to come to terms with those limitations. I mean, let me turn to our student.

[00:56:49.20] Question please.

[00:56:51.87] STUDENT: Hi, my name is Jacob. I first thank you all for speaking. I find it very interesting just hearing from all of you who have seems very different backgrounds and interests and perspectives.

[00:57:03.99] But I just want to ask you Patty, if you could talk a little bit more about that time where you were navigating in the middle. I guess, what I'm curious about is even though you are positioning yourself in the middle, weren't the people around you still aware that you were still on the side of revealing the truth and talking about what happened?

[00:57:25.59] PATTY LIMERIC: That's a-- I think that's a great question. OK. So did I really ever have-- did I convince anybody that I had repositioned myself? That's part one of the question. And I think that by repositioning myself that I was an external performance.

[00:57:46.09] And then it became an internal performance because then I was listening more to the different sides. Then I was never as clear about thinking this is my ringing conviction. So I ended up getting as confused internally as I was externally. I also got many better stories to tell because I was hanging out with people and learning things.

[00:58:03.34] And I'd do anything for a story. So that was true. But I think you can still watch me in public struggle. And that probably is the basis of my credibility. So in Western American history. Now many, many, many, many, many, many historians use the term "settler colonialism" to describe what we used to call westward expansion.

[00:58:23.65] And I don't go there because in my opinion that framework is supposed to give more recognition to the dispossessed Aboriginal people. In fact, it kind of squishes them into victims passive victims. So I don't really care to be part of that. But it also homogenize the settlers.

[00:58:39.40] And I'm not interested in that either. So settler colonialism now is in some ways maybe it was what came after my book, Legacy of Conquest that we will condemn the settlers and see them as-- haven't said they are responsible for the displacement of Native people and for ongoing inequity.

[00:58:59.19] And that's all there that has to be. But they're very diverse people. And so you can watch me in discomfort and struggling to get my footing when I take on that term settler colonialism. And say I can't join you in that. And it's not because I am now wearing Western wear. It's not because of that is that I really don't see a pendulum swing as a satisfactory.

[00:59:26.02] I mean, a pendulum passes through the middle and then it's off again to an edge. So I just feel that when I am able-- I'm going to just say this it's preposterous. But when I am able to monitor myself and speak honestly about what seems flawed in the various sounds coming at me from different sides. And still trying to reconcile and still try and listen.

[00:59:51.16] I think in some way I'm serving my troubled nation which is a ridiculous thing to say because you can see what an impact I've had whatever it was. Just imagine how bad the nation would be without me doing this? So that was a really silly statement.

[01:00:04.15] And I'll deny it if you ever quote it to me. But--

[01:00:07.60] MEG LETA JONES: No one will ever know. That's fine. Great, Thank you. Can we--

[01:00:11.64] PATTY LIMERIC: Yeah, that was [INAUDIBLE].

[01:00:13.24] MEG LETA JONES: Yeah, lovely question. Just one in the middle of the room.

[01:00:21.31] STUDENT: Hi. It seems like a lot of discussion both this morning this afternoon about disclosure and accounting it's a larger problem of discovery and litigation as it is. In this case, government, the public is trying to find out what personal data you have. And now the EU under the GDPR is requiring mentor disclosure.

[01:00:48.85] Everybody's gearing up in this country for expected more regulation and mandated disclosure of personal data and the data behind an algorithm intelligence driven machine making. But like in discovery litigation and like I think Andrea who represents companies is that everyone realizes they have valuable data.

[01:01:19.15] They're being required to disclose it. Almost universally they never want to disclose it. And this debate now seems to be identifying why it's impossible? Why it's very expensive to do?

[01:01:37.33] Why the data is all dis-aggregated in different databases and in filing cabinets? And they're afraid that they're going to disclose proprietary information, trade secret information, information, they don't want their adversaries competitors to have or disclose HR problems in the past and open up the door to more liability.

[01:02:03.77] So it seems like we're going to go through a long phase here of data companies and platforms fighting any mandated disclosure because they have a whole host of reasons why they don't want to do it. The EU has bitten the bullet. And they're going to requiring it although we do hear that there's a lack of budget or data attorneys to force disclosure.

[01:02:34.05] So they're going to go through that phase. But I would just hope that all of the players get on board. That they're going to have to do it. And rather than drag this out for 20, 30 years or whatever and do it in dribs and drabs. Because I think that they're sitting on a mountain of data.

[01:02:57.17] And their business model is predicated on making billions of dollars on this valuable, valuable data that is personal data. They're using it to market and sell advertising. And how can they avoid admitting that this is valuable, valuable personal information that's driving marketing, decision making, personal lifestyles?

[01:03:20.81] And that I think the US should finally come to grips and force this that it's being misused. Being misused for proving insurance,

mortgages, loan, and credit ratings. And that people have a right to find out what they have on file and what form, in what detail? So they can start to control it and their lives are being driven by a mountain of data they can't get access to.

[01:03:54.54] MEG LETA JONES: I'm going to suggest that is a question for Emily. Emily, is there-- does that sentiment land at Meta? Does that sound like how you guys are coming to terms with this or are there parts of that you would take issue with and say, "Look that's not really how we're seeing the regulatory landscape."

[01:04:29.95] EMILY MCREYNOLDS: So I think there's a lot to what you just said in terms of the variety of legislation regulation that is happening and the implications for personal data and how it's being dealt with. From where I sit, as more of a research expert, I think we're here because-- I'm here because I think transparency is important.

[01:04:55.59] And I think it can be impactful. I don't think it is the end all and be all that it's the perfect solution. We've heard that all day. But it's one of the tools that we have right now to address some of your concerns.

[01:05:12.24] ERIC GOLDMAN: Can I come in? Just a couple of things I think that your remarks really highlight for the audience the spectrum between privacy laws as a protection for individual data. And what I've been focusing on the transparency to the editorial operations of the services, which I think is a different qualitative issue than the one that you were actually focusing on.

[01:05:35.85] And one that I would encourage you to potentially distinguish and say, "I understand that I should have the right to know what is going on with respect to my data. But I don't have the right to know what's going on in the head of an editor when they're making an editorial decision." That's something that's just not my purview.

[01:05:52.23] The other thing I just want to mention is that the movement today is towards forcing companies to make these disclosures before there's any litigation at all. And so you were talking at the beginning of your remarks about discovery. And I just want to point out the differences with discovery.

[01:06:05.73] Discovery only occurs here in the United States after there's been a complaint that's been filed. That's subject to things like rule 11. And that the judge has not granted a motion to dismiss, saying "I think there's enough merit to let this case get to discovery."

[01:06:20.28] And then within discovery there's rules of engagement. Like there has to be relevance. You don't get all information. You actually have to get the information that's relevant to the legal violation that's in the complaint.

[01:06:31.56] What we're seeing with the movement towards mandatory transparency inverts all that and says, "We don't need to get to discovery to find out. We don't need to show that there's a legal violation. We get to see everything even if there's no legal violation whatsoever. And so it's a qualitatively different thing than discovery."

[01:06:51.39] And it actually helped remind just how broad and ask it is. That doesn't mean it's a bad ask but it definitely is a broad ask. And that raises a lot more concerns about why are we requiring this data? What is the costs of this? What are the risks to disclosure when there's no judge supervising this battle between the parties?

[01:07:13.56] Last thing I'll say. You did say you're going to have to do it you're sitting on billions of dollars of revenue. I think you may have had one company in mind but I will point out that the ecosystem is really quite broad and there are many services that are not sitting on billions of dollars. Are not sitting on billions of pieces of people's data. And we should not ignore that they are going to have a qualitatively different decision than the giants.

[01:07:37.11] MEG LETA JONES: Thank you. Can we get Jeff a mic. Jeff can you raise your hand?

[01:07:47.47] STUDENT: Yeah I just quickly wanted to react also to the previous question and give the European perspective, if you will. In the whole range of laws and proposals that we've seen suggest in the last couple of years in Europe as I said before, there's this common denominator of transparency and compelling data access. I think how I read it, I read it like in across these different frameworks there's to me a clear like intention to break up to not have businesses, build an entire business model on data in itself.

[01:08:28.49] And to force companies or to not silo off their data and basically to have business models form around what you do with the data rather than hoarding data if that makes sense. And I think that's an interesting thought experiment. I'm not sure where I'm standing on the European Commission's perspective here.

[01:08:55.09] These business models that we've seen emerge in the last 10, 20 years, we've come to accept it, it seems as a natural law or something that these companies should have a right to shape their business model around this. But I think it's an interesting thought experiment to see like maybe that's not OK.

[01:09:14.74] And maybe data should run freely. And it's more like what you do with the data.

[01:09:24.70] MEG LETA JONES: Who else has a question? I think we have time for at least one more, right?

[01:09:28.42] STUDENT: Actually, I got one.

[01:09:31.00] MEG LETA JONES: I think you're a long way from a mic. Here we go.

[01:09:40.72] STUDENT: Yeah. So this is to Eric but also to the other panelists. First of all, I think I mentioned this in a one on one conversation. It's fascinating to me that the chilling effects arguments that you're making around disclosure and editorial policies are like the same foundational arguments that have been in place in both Supreme Court cases and in private litigation around the anonymity of speakers.

[01:10:10.54] And so it's just fascinating to see these arguments want to talk about narratives. These arguments about chilling effects and the benefits of privacy for communication. Now, being that they get applied selectively. They get applied to-- we see this in FOIA too. Like an open records laws where you have an open records law that will say we need a disclosure in the name of Government Accountability.

[01:10:34.36] And the exception there is going to be for deliberative conversations before you get to the final policy. We don't want to chill the making of policy. And so we don't allow for disclosure there. Yet when the same argument is being used about personal privacy, it dissipates.

[01:10:50.65] So that's more of an observation than a question. The question I had was if there's this pull of editorial decisions clearly speech transparency becomes a chilling effect in a way that's so tightly intertwined with actual traditional historic speech that it's problematic. And then on the other side, there's something once we get into privacy or other places where information is being exchanged as opposed to there's this traditional historic editorial context, there's room there for transparency and for disclosures.

[01:11:26.41] Whereas the boundary drawing? Like where do you decide? And I guess it's back to Amanda's work too. Like where do you decide this is unacceptably close to call for First Amendment values and interests versus actually the transparency is serving core First Amendment values even if it's not something that's required under actual First Amendment Law?

[01:11:52.78] ERIC GOLDMAN: Yeah. I think it's actually helpful to analogize to traditional publishers for a moment, which is always a little bit dicey. But walk with me for a moment, and then we'll see if it blows up. Think about the integrity of a traditional publisher's newsroom that we put severe limits on the government's ability to come into that newsroom, to grab information from that newsroom. Because the simple presence of them there put at risk a journalistic function.

[01:12:25.06] It put the risk that the journalists couldn't go out and gather information that might be sensitive, that might be under a shield expectation if the government can just come and grab stuff. And because of that, we generally haven't seen the kinds of demands for

exposure of editorial decision making. In the traditional world, we're now only seeing today in the internet world.

[01:12:54.04] And what I find so fascinating about that is that traditional publishers almost always become concentrated markets. That's a feature of all media niches is that they become concentrated. So there's always people with market power in those niches who have had huge impacts on the conversations that fuel our democracy.

[01:13:15.92] If you think about the local newspaper Circa mid 1970s. If they ran an editorial against a politician, there was very little that the politician could do in response to that. They had to scramble to find alternatives. And yet we accepted I think tacitly perhaps. Silently, that we couldn't require the newspaper to disclose how it decided who to endorse and why they decided to endorse and where they decided to put that story?

[01:13:50.17] Front page, editorial page or somewhere else. Which is accepted that those decisions were not in our purview to be compelled. If we didn't trust them, we could ask questions. If we could drop our subscriptions we could protest. But we accepted tacitly that those were just off limits. And to me, I feel like we're doing a redux of all that except we're bending all the rules.

[01:14:12.34] It's like OK there's a thing called an editorial function. These are the content reviewers and the public policy and the product policy and the Trust and Safety teams. They're all working together decide what do we want to publish our audience. Tell us everything. This is all fair game to the public and without it democracy will fail.

[01:14:32.81] And to me I can't wrap my head around that dichotomy. That doesn't mean that there aren't differences between the two. But I don't find any of them persuasive enough to say that we would choose to allow the government to intrude into the functions of these publishers, where we would have never accept I think in the other types of publishers.

[01:14:53.29] MEG LETA JONES: Hannah, do you have-- I can see you thinking on your little box up there. And I can't tell if you'd like to hop in. But I'd love you to if you do have a response to Margo's question or Eric's response to it.

[01:15:12.81] HANNAH BLOCH-WEHBA: I guess I have a small footnote to Eric's response, which is to say it's hard. I mean, this is not fully thought through. A bad thing about my face is that my thinking is visible. So my thinking is complete on this. However, I will say, I think that we over the last century, have seen the traditional news media make a series of editorial discretion arguments about different forms of regulation that have not always been successful.

[01:15:46.96] And so we've seen this argument about editorial discretion be made, for example, in opposition to antitrust law or to

labor law, and courts have rejected it. And so there are limits to the notion that editorial character creates legal immunity. And the question is going to be where those limits lie?

[01:16:14.11] And it's not a settled question with respect to either the traditional media or with respect to social media companies or platforms or any of the data driven business models that we see emerging today that also are donning the mantle of editorial discretion. So to that I'm thinking about here are Clearview AI which exists to be a social-- like to be a search engine but only for government customers.

[01:16:44.74] And says and has a First Amendment right to do all sorts of privacy invasive things even though it's essentially only a government contractor. And the other one I'm thinking about here is-- just slipped my mind because my thinking was totally incomplete on this. So I think that there are potentially areas where the law is not yet settled on these questions.

[01:17:15.77] And so thinking about where it should take shape is an important exercise as we enter this next stage of policy making. And the answers are not obvious to me.

[01:17:35.51] MEG LETA JONES: It's a perfect way I think to end the panel. Thank you, Hannah. And Thank you all of our panelists. Please help me in thanking them.

[01:17:42.80] [APPLAUSE]

Keynote: CO Senator Robert Rodriguez

<https://www.youtube.com/watch?v=xb25m0vgEol>

[00:00:00.93] MARGOT KAMINSKI: If I said that my panel was my favorite panel, this is one of the conversations I'm most excited about today. In just a minute, we'll get started. But for those of you, who are here, I'm delighted to introduce Senator Robert Rodriguez, who was a prime sponsor of the Colorado Privacy Act, or CPA, not to be confused with the CCPA, or California's Privacy Act.

[00:00:28.71] So what I'm hoping, we will hear about today, in just a minute, is a little bit of a story behind an actual privacy, transparency law, and the rationale for why such a thing is enacted. And a little bit more information on what state legislators are thinking when they put in place actual transparency requirements. So maybe give it another two minutes, and we'll get started?

[00:00:52.09] ROBERT RODRIGUEZ: Sure, sure. Just for the record, I am not an attorney. I only play one in the Capital. I've been overwhelmed by this, so, hopefully, this will be a little bit of a downplay, for you guys. And I'll dumb it down, and I can just tell you

some more dirt and gossip of the legislative process. Good dessert time.

[00:01:15.92] MARGOT KAMINSKI: I should also point out how grateful I am, that Senator Rodriguez made time for this, during a very busy election cycle. So big gratitude on that front

[00:01:25.82] ROBERT RODRIGUEZ: I've only taken a couple of ballots, so if anybody needs their ballots dropped off, I am available to drop off.

[00:01:29.46] [LAUGHTER]

[00:01:31.25] I was asked to go check out the Student Center, to see if people were dropping off their vote.

[00:01:35.60] MARGOT KAMINSKI: Vote, make sure you vote. All right. So I think, let's get started, and people can trickle in if need be. So, again, it's my absolute joy to host Senator Robert Rodriguez. We'll, again, do a similar format of a Keynote presentation first, followed by some discussion with me, followed by an opportunity for, you all, to ask questions and get answers.

[00:02:04.74] ROBERT RODRIGUEZ: Yeah, thank you, all. It's an honor to be here. Thank you, Professor, for having me, and, you all, for being here. I got here a little later in the day. My intention was to show up, and listen to the whole day's presentation, but, as I got up this morning, at 6:00, a little bit of snow and a lot of accidents. So I didn't want to ruin your presentation, by getting in an accident, and not being here to provide this to you. So I'm here now, and I came safely up. So thanks for having me.

[00:02:29.04] I'm not a lawyer. Mostly, I've been in the election-- in the Senate for four years. I came in, in 2018, started in 2019. Mostly, worked in criminal justice, reform, small family business, worked in the mental health and substance abuse field. But also did a lot of work, in my couple of years, with consumer protections. My first year, I came into the legislature, I worked on a pretty contentious bill that was there before I got there, which was the remote notary bill. Which was before its time, with COVID.

[00:02:58.11] It was something that they were trying to expand on. and it took me two years to pass, just because of some of the arguments. But one of the big arguments was, fighting with the real-- with the trust companies, and the deed companies was because they're recording the editorial act. What are they doing with that information? They're recording it. Are they selling it? You have access to the documents? One of the trick questions was the definition of sale, which was a big issue, that I didn't realize how much it was.

[00:03:26.19] And a little history about me. My wife is a privacy person and has done it, and I got into that with her. And I learned about, well,

there's a lot of different ways of what sale means, and it's trading. And we thought it was for money. Well, there's a lot of other definitions. So that bill got done. And, because of that, I decided to dabble into consumer data privacy.

[00:03:47.29] So this was in 2019, we started working on it, and we were going to introduce that bill. And I built a coalition. The people that worked on the remote notary bill with me, were my house sponsors, which were, one was Republican, one was a Democrat. I'm a Democrat, for the record. I advocated for a Republican, in the Senate, to work on with me, who had done some previous children's privacy stuff, in the past.

[00:04:09.75] Believe it or not, there's a little bit of a privacy caucus in the legislature, the discovery I've had. And I've worked with other states, and talked to other people, even after we passed this bill. His privacy is very bipartisan. It's not a monolithic thing, for people. The nuanced arguments for it are, but it was a good coalition to build.

[00:04:27.60] The first time I had a meeting with them, we sat down in a room and said, what do we want our bill to be? And I was-- I'm probably more of a opt-in, slash, right of-action person, which, I knew, having a bipartisan bill, I couldn't get done. But that's what I wanted, and I went in with my colleagues. And my Republican colleagues are like, I believe we should have an opt-in on everything, I don't want these people with their refrigerators in my house.

[00:04:51.84] And I was like, I love you guys, this is great work. I was surprised, and we started working on a bill. So at the time, this was early 2020, and we started looking at policy. And California had just passed their bill. And we started to go, well, we started talking with lobbyists, we're. Going to do it and the discussion got to be, please, don't do California. Because, at the time, California was a ballot initiative, and it was a kerfuffle of mass, of people having to change it and regulate it.

[00:05:20.70] Some of the lobbyists were probably saying, you should do Nevada's. So I went out and looked at Nevada's. And it's like, well, Nevada excludes all the carriers and the providers. And I was like, oh, of course, you want me to do that bill. So I was like, no, we didn't do that bill. So we did a little research, and we came up with Washington's version, which never had been passed. But it was probably one of the most balanced and thought-out bills that we had.

[00:05:40.30] So we modeled it after Washington Privacy Bill. We worked on it for eight months. We took that bill, went a little stronger. Like I said, my wife and me, were the first starters of drafting it. And my wife works in health care privacy. And the fights were going to be, well, this is untested, there's no proof, there's no way to do this, we can't do it.

[00:05:59.82] So we modeled a lot of our first draft on HIPAA wording, which, they didn't like that, either. But that's for the end of the story. So we did the bill, and we were going to introduce it. I think it was going to get introduced in the legislature in 2020, on March 15, it was going to-- right across the desk. opt-in, full bleed knowledge, no right of action, but the AG enforcement. And I can talk about that, in question and answers, if you'd like to.

[00:06:25.68] So we were getting ready to do it. And that was the day that they shut down the legislature in the state for COVID. So we didn't get our bill right across. They pulled it off. We came back after COVID, and everything was shut down, and everything was emergency. So the priority was not to do this bill, so we didn't introduce that bill in 2020. So we moved on and we committed to work on it again, for the next year, which we did.

[00:06:49.77] The next year, we met with a lot of business leaders, and we did a lot of crafting. And we worked with a TechNet and a lot of tech companies, who build conglomerates together, that worked with us. And we worked with Consumer Reports, ACLU, some people from California. A lot of people were dabbling in it, but probably the biggest advocates were the business community, the chambers, and the TechNets of the world. Which, after our bill, we have a TechNet in this region.

[00:07:15.46] So if anybody is looking for work, after that too, we started that. Nobody we can say Democrats don't create jobs.

[00:07:21.26] MARGOT KAMINSKI: [LAUGHS]

[00:07:22.92] ROBERT RODRIGUEZ: So that bill got introduced, and we worked through the process. And a lot of the process was trying to build a balanced bill. As an advocate for opt-in, I believe that is good policy and a private right of action, but, also, looking at GDPR, and as somebody who is geeky enough, that reads the privacy statements and the statements that come in the bill. I even, now, that our bill is passed in California, is passed, I don't know how many of you actually read the privacy, accept cookies, accept tracking, which, I read them too, and it's, yeah, it's kind of sad.

[00:07:55.71] And I actually think those are dark patterns, which we could take it, is like, yeah, accept all or go into this multi thing that's going to tell you how, if you check this box, we're going to enhance your experience, right? So we tried to be balanced with the business community, always knowing, going in, my goal has always been the end user as a consumer. We fought very hard. My colleagues fought very hard. We got this bill out of the Senate unanimously 35 to 0, bipartisanly.

[00:08:24.57] Some of the mistakes, I did some amendments that I probably shouldn't have done. But as you go through a process, you don't learn everything. I probably, I could talk about, and if you ask

questions and answers after, regrets that I didn't do in the bill. Or mistakes I made, that I had to honor. One of them was probably the GLBA exclusion.

[00:08:43.17] I probably went too little too far on that, but, because I made that commitment, I had to stick to it. But it's hard to get these bills done with the amount of force because you have a few legislators, a couple of advocates, which is probably Consumer Reports, and that. But you're going against the whole business industry, which, they all believe in this stuff, but when you dig into the amount of data, and the amount of stuff that they collect on you, and the amount of-- and the fights I had, whether it was the LexisNexis's of deleting the data, or them.

[00:09:13.14] The biggest pride I have in this bill is that we have a global privacy switch, which is the most uniform thing in the nation, which was exciting. And for us, it was a very exciting thing to do, in the bill. But we worked on a lot of collaboration with stakeholders. My intro to the bill, which I thought I'd pull up to read to you when I had to go and present it, which was, I thought would convince everybody I was excited about this bill. Maybe it sold it, maybe it didn't, but I'm just going to read through my intro when I did this bill.

[00:09:42.67] There's no overreaching policy rule, the federal level, that applies universally to US resident data. So the states are having to pass their own product for consumers, to protect consumers. This is exactly what this bill is about. The protection of consumers and affording them rights around the collection, use, and disclosure of their data. Every week, privacy is a major theme that is in headlines of major news stories, Facebook, Cambridge Analytica.

[00:10:03.94] April 2021, Facebook, 267 million profiles listed for sale on the dark web, for \$600 a word. April 27, 2020, Nintendo, 160,000 player accounts hacked. Often, others, such as Expedia, Pfizer, FireEye, Barnes and Noble, Staples, Instagram, TikTok, and YouTube, in 2020, just to name a few. This bill puts several guardrails into place for consumers to better understand what data companies have about them, and to give them some control of that data. As technology progresses and big data is readily available, their data is being used for targeted advertising for products and services.

[00:10:41.09] I had a story after COVID. I had went and got my COVID [INAUDIBLE], and you go to Labcorp to get your test. And to get my results, I had to log on to the Labcorp website. And through that process, I had to verify who I was. And some of the security questions had asked me, which, I'll go over. And it was four questions. One of them was like, what county-- what month-- what day-- what month of the year is Corinne's birthday, and who's my mother.

[00:11:07.07] So it gave me options. And I was like, all right, I probably fill out a form, they have that information. The second one was, which cars do you own, have you ever owned out of this list, which, none of

them were the ones I owned. So I was like, OK, that was just a guess. Well, the fourth question was, what is the county of residence for this address, which was a rental property that me and my wife owned? And it wanted to know what county it was in, and I was just like, what?

[00:11:32.65] The creep factor of the information that these people bought. And, like I said, my wife does privacy, and I called her, I was like, why would they have that information about me? She's like, that's public information, people buy and sell that stuff left and right. Which, a whole other discussion about the access to that public information, and another bill. Maybe, when I run for Congress, I'll run on that.

[00:11:51.46] So that was another thing for me to enforce. But it was predicted in 2020, 1.7 megabytes of data is generated every second, for every person on the planet. For a frame of reference, 1 megabyte is equivalent to two reams of-- or 1,000 sheets of paper. So 1.7 megabytes is close to 2000 sheets of paper that's being collected on you. I heard discussions earlier about this data is being banked, because they may find some future use for it.

[00:12:19.09] We put some data minimization in our bill. The arguments they have about the unlocking of data, maybe they just shouldn't keep it, and they wouldn't have to worry about getting this stuff. So bill was a huge lift for us. And I was very appreciative of the process, and my colleagues, for doing it. It's opened up a lot more discussions for me.

[00:12:40.93] When we first planned this bill, we were thinking about including biometrics and a lot of other stuff. And just doing research on other bills, it's just too big a monolith of policy to carry in one bill. And if you ever deal with legislation and stuff, it's hard to pass gigantic, sweeping bills. It's the old adage of how to eat an elephant, it's one bite at a time. And if you look at policy getting passed, it's usually one piece, because the big bills are so complicated.

[00:13:08.86] And this bill is still complicated. I didn't get everything I wanted in this bill, and probably neither did the AG. He came in and tried to amend it, and do a lot of stuff. And I was like, this bill won't pass the way it was, they wanted to get more stuff into children. We had negotiated a lot of that away. But it was an honor to be a part of some policy that will give Coloradoans rights that not a lot of other people in this country, or the world have.

[00:13:34.33] It's not enough. It's a lot of work that I'll be digging into, more in the future years, whether it's AI, or discussions today, or biometrics. This bill was so hard on me, and I married this bill so much that I've kind of have some PTSD about doing another policy bill. It's a lot of lift. Like I said, there's a lot of people passionate about it, but it's not the people that are paying thousands and thousands of dollars, of people in that building, to tell other people this is just going to kill-- every bill is going to kill the industry, as we know it.

[00:14:07.12] Every policy is going to hurt everything, and we constantly find it doesn't. And to many of the statements here, not all actors are bad actors. There's companies out there that try to do the right thing. They have a responsibility to make some money. Some of the pride I have about this bill is, it's the first one with the global privacy switch. No other state had put that in.

[00:14:29.41] We are the first the only state in the country that includes non-profits. We'll see where that goes. It's undiscovered country for all of us. I'm nervous, but we're an incubator of tests. So if I have to change it, I'll change it. But right now, some of the digging I did, and some of the research I did on nonprofits, are a big use for people to hide ways of getting privacy, and that's how they fund. I had a lot of people chasing me about it, with some of the news articles and the web people.

[00:14:59.30] And I did an article for-- I can't remember if it was The Markup and stuff but they did an article on nonprofits, and why I did it. And for me, it was always like, I don't understand why not. But they had some web tools, that they would track websites, for a lot of these nonprofits, and how much cookies, and tracking, and where they went, that was on their websites. And as people were emailing me about them. They had no idea that their websites were tracking that much information.

[00:15:22.59] So I was like, well, we're really-- I was like, why are you doing this to us? And I was like, I don't know if you-- we capped this at 100,000 records or higher not to stifle small business and innovation. We put exclusions for the health and safety and science stuff, trying to be smart about it. But at some point or another, this will catch up.

[00:15:45.08] The tech industry now I think more as this policy is changing, we're seeing more information with the tech and the cybersecurity people getting involved in privacy stuff. It's becoming more and more-- because I see policies-- I ran a bill that you have to accept cash. If you guys go around, nobody's taking cash anymore. And credit cards are getting processed. It's more information.

[00:16:03.41] They're tracking about what you buy and sell and what you do, or smart refrigerators that know when you open the door or when you get home, or laundry machines that know when you're doing the laundry, if you're doing them in the middle of the night or the middle of the day or when you're home and when you're not. I stayed up for a while when you think about that. I don't have a tin cap on, but I do think about all the things that get caught up with all the things you turn on.

[00:16:29.06] The biggest argument I had when I ran this bill was probably the fight between now Meta and Apple, which was the right to track app that was put in. And it was probably one of the biggest sales that I had with my colleagues on this bill. And the data that I could provide was that when you were being asked if you would allow

apps to track you outside of their application, it was about 4% to 6% of people who were allowing it. And to me, that's why the industry doesn't want this policy.

[00:16:58.67] And even with the global privacy control, which I think they can make-- they're like, it's untested data. It's untested thing. We don't think we could do it. I'm like, if it made you money, you could probably make it work. So there's a lot of people mixed bags. I think I collaborated most on this bill with Microsoft, who I got a lot of grief for working with them because they're the big behemoth on the corner because they're gateway to a lot of data.

[00:17:25.55] But at the end of the day, the enemy of my enemy is my friend. And while I may not agree with everything they all do, sometimes you have to pick your battles and who you work with to do this stuff. So the journey has been great. I've met a lot of great people in this process. I'm excited to have people that are probably as passionate about this as I am that I had never known. I've got to speak at multiple events. Being at this is like I'm kind of like a king of the geeks I guess on privacy law in the country because there's so few of us and it's not exciting. But I have that going for me.

[00:18:00.80] And I've met so many great people that want to work on this policy going forward. And as we get more and more reliant on the technology we have, which I had the GPS to get here. I understand what I'm giving up with things, but most people don't. When I would talk to people when I was running this bill, the older people have no idea how much privacy they don't have, and the younger people just assume they have no privacy already.

[00:18:25.02] So it's such a nuanced conversation. And I would bring it up with the young kids. It's like, what are you going to do someday when you're older and you're applying for insurance or life insurance or health care and it's like, well, we noticed that you tend to go to fast foods an awful lot. You eat a lot of cheeseburgers or greasy bad processed-- that's going to affect your premium. And geek out or not, that's the kind of stuff that will eventually be available for people.

[00:18:48.09] So just being here for a consumer for me in this bill that we ran and doing interviews and other states that are looking at it. The only advocacy I do for them is to push the envelope farther than what I did. I know the federal government has been working on a policy. Whether it'll pass or not, I'm not sure how I feel about their preemption wording on it. But they need to do it.

[00:19:09.91] I'm working with some other senators. Connecticut passed a bill very similar to ours a year ago, and now we're starting to think of ways because the fight with data privacy is that it's so hodgepodge across the state. Businesses and industries comply with multiple states policies. So now we're going to look at a process of maybe getting multiple states together to look at some uniformity,

which hopefully will be an argument why the business communities can't support a policy that we're trying to streamline it for everybody.

[00:19:36.99] There will always be nuances based on states. But at least with uniformity of language definitions and processes, it'll be good. I don't know if there's any questions or a pause and any broad questions anybody wants to get or any gossip of the legislative process, but I'm happy to take some.

[00:19:55.26] MARGOT KAMINSKI: Oh my gosh, so much. I'm going to start with this. So first of all, this is already fascinating. When I teach about the various privacy regimes, I typically characterize the Washington Privacy Bill, the one that wasn't passed, as the Microsoft bill because that sort of-- how it fell apart in Washington State was that Microsoft effectively helped draft it, and NGOs in Washington State were not very happy about this. And as somebody who studies the GDPR, was tracking the CCPA-- we are among privacy geeks here, by the way. It's happening.

[00:20:35.84] It was fascinating to me to look at the Washington bill and say, this is the only thing on offer right now that actually tries to track the GDPR. And the political economy of it totally makes sense. Like Microsoft has to comply with this thing because they're a big global company. They would love for some state senate to basically enact it to impose the same costs on their competitors.

[00:20:57.63] So yeah, the enemy of my enemy is my friend. So I've seen that be picked up. And it's really interesting to hear you talk about that and and acknowledge that that's deliberate. It's not necessarily that Microsoft is showing up and saying, hey, this is the version that should happen. It's like this is a version that actually is like the backbone, is pretty OK.

[00:21:21.77] And I'd love to hear a little bit about the inside baseball process of taking that backbone and saying, what can we do with it? What can I put in there that's going to be more than this? What can I put in there that sort of got the initial buy-in, but I can kind of take it to a place that's definitely not what showed up on the table initially?

[00:21:43.79] ROBERT RODRIGUEZ: That's an interesting thing because like I said, working with the tech nets and the larger tech groups that Microsoft was a part of-- but you talk to them, there's a lot of anger and hate amongst them because of this. And for them, Microsoft is the big giant on the table. They have one of the biggest operating systems, they will have a global privacy switch, they will have the ability to track what they get because everybody gets their data on their platform.

[00:22:10.22] The carriers the CenturyLinks, the rise, they're the gateways to everything. And they get even more data than the provider depending on what they use, if it's a phone or your internet, or anything else. They were pretty collaborative on most of stuff. They

were a very useful resource in the technological wording stuff that you get into because if you-- and you guys have read these bills. If me, who had somebody as a resource to learn this policy stuff and to talk about it, as a legislator, a lobbyist, or anybody that reads this bill has no idea what this bill says, what's good or bad.

[00:22:48.86] I was trying to put in a good strong definition of biometric data in the bill. And I put a very strong version tried to get it in the house that included gate and a lot of stuff because they wanted to exclude facial profiling, which was my fight with Facebook. And I was like, this was at the time, when Facebook would tag you. And they got it taken out because I had people arguing that it was going to create biases and all the other stuff. And I was like, that's not what this policy does.

[00:23:15.23] Because they don't understand the nuances of the policy, it was hard to get through unless there was a lot of trust. So most of the people were pretty collaborative. Microsoft was good. And the tech companies were pretty good too. The policy was very broad when we first introduced it and we went all in with everything as hard as we could go with it.

[00:23:34.16] MARGOT KAMINSKI: What was the initial private right of action, just out of curiosity?

[00:23:36.71] ROBERT RODRIGUEZ: Well, I never did a private right of action because I would have never gotten that. The reason I did not do a private right of action, as much as I'm a pretty big consumer advocate, is you can't get private right of actions bills probably through just my caucus, let alone Republicans. We see a lot of that stuff, whether it's other types of negotiations or-- I can't think of the word now, but we've had big fights over right of action.

[00:24:01.98] So I knew I could never get that in my policy, so that was never an idea for me to do. It was my concession for me personally to have a bipartisan bill because when you have a majority of 17 or 18 in the Senate, if one side completely hates it, two or three people can completely get a bill. Manchin, Sinema, Congress. So my strategy was to pass a bill bipartisanly because for me not-- if we talk about Washington, Washington's bill always dies because the AG and them wanted a private right of action and the sponsor didn't. So weird argument.

[00:24:37.80] And I told him multiple times like dude, if you pass that bill with that, you will be the trend setter across the country. And it's a nuanced argument because I talked to somebody in Florida that was running this bill too as well who tried to put a private right of action. And for me being in Colorado, a private right of action, there's too many lawyers. I think it creates jobs for everybody, but it is what it is.

[00:25:02.56] But in the South, Republicans are trial lawyers. And they were more up for it than I would get it through here. And here, trial

lawyer is an evil thing and they're here to ruin industry and just raise costs. It's an interesting argument. But then you go to the South, and they're like, oh no, we love taking on big business and who they-- can't remember the name of the Congressman that's in the Senate. That's a trial lawyer that's a Republican. Lindsey Graham. Big trial lawyer advocate. You wouldn't know it, but he is a champion for trial lawyers in Congress. So live and learn.

[00:25:32.98] So that part of the bill I could never do. And the opt-in, we tried, but we knew we wouldn't get it through our caucus. And by the time we had spent a year because we were going to drop it with that the first year, if we'd have worked on it in the summer with that in the bill, they would have lobbied it before we got to the floor. So we took it out in the interim to go back to what we had.

[00:25:58.42] I think Senator Carlisle is the grandfather of all reasonable privacy bills. California's has gotten much better. At the time when we did it, it was a little note. I think when I talked to other people in states when they're looking at privacy, if you really want a good privacy bill, you put it on the ballot, just like California did. You will get opt-in, you will get everything because there's nobody that doesn't get-- privacy polls at like 80% positive. It's just who's got the money to spend to get it on a ballot.

[00:26:27.13] MARGOT KAMINSKI: Yeah, they're still sort of a pet a pet project of mine would be to try to revive conversations about state constitutional amendments around data privacy too.

[00:26:37.21] ROBERT RODRIGUEZ: That would be fun. Then you need 55%. You could get it on this field. Let me know when that guy-- if you meet that person, I'm happy to help you.

[00:26:47.08] MARGOT KAMINSKI: That's awesome. I also want to go back to-- I'm not even at my questions yet. I want to go back to something you said about having some regrets. What were the regrets of these compromises that you made that you think you actually probably didn't have to?

[00:27:01.26] ROBERT RODRIGUEZ: Not being a lawyer, one of the first concessions I made was my tweaking of the wording, any entity connected to the Gramm-Leach-Bliley Act. Words mean something in contracts and legislation. It was one of my first big ones and I accepted the wording. And I didn't find out until somebody did an article on the bill that I completely gutted the financial sector. And I yelled at a lot of people after that. But I also had to own the fact that I made that mistake. So that was one of my big regrets I did on it.

[00:27:39.57] Some of the other ones is that I didn't push to exclude-- this bill had government covered in it until the house. I had government in this bill until the house. I got yelled at by everybody. It's like, how could you? This has been introduced. You didn't pay

attention. And probably excluding CU and CSU. Again the lobby, but yes.

[00:28:01.20] MARGOT KAMINSKI: Yeah, that's also fascinating about the university lobby.

[00:28:03.27] ROBERT RODRIGUEZ: I should have sent you in. I was like, no, we can do this.

[00:28:05.04] MARGOT KAMINSKI: Yeah.

[00:28:05.37] [LAUGHTER]

[00:28:06.63] Next time. Yeah, so then returning to my conference relevant questions, I think it's not necessarily intuitive for most people that transparency is a core principle of data protection. And so when you were talking to your colleagues, or you're talking to a constituent and they're thinking that you're writing a bill that's a privacy bill that will let them fully control information-- and I heard control in your preamble, and control is a big part of this, but how did you characterize the transparency provision? How did you explain to people that that's actually core to or connected to data privacy?

[00:28:45.93] ROBERT RODRIGUEZ: I think, you've got the five things. You have the right to delete, right to correct, right to opt out of sale, right to collect what they sell on you. I had it up on my phone I don't remember the fifth one off the top of my head unless you do.

[00:29:01.15] MARGOT KAMINSKI: What was it, correct? Yeah, I think it is correct.

[00:29:02.79] ROBERT RODRIGUEZ: Right to correct, right to sale, right to opt out, right to delete, and there was one other one,

[00:29:09.54] MARGOT KAMINSKI: Was access.

[00:29:10.26] ROBERT RODRIGUEZ: Right to access.

[00:29:10.92] MARGOT KAMINSKI: Yeah, that's the big one.

[00:29:11.58] ROBERT RODRIGUEZ: Yeah, which an interesting note which gets into some ethics questions that popped up earlier. There were people that tried to amend the bill to allow-- I think our bill allows you to pull your personal records once or twice a year. There were people that wanted unlimited, which would have been a humongous fight with the tech industry if they had unlimited. But there's companies out there that will pay you to sell them your data.

[00:29:33.30] And there's discussions federally, I've heard it from Congress people stuff that get it. The argument is at the end of the day whose data is this, and should you be able to sell it? There's apps.

There's a Colorado based company that pays to track what you buy and sell and shop on. And that was somebody who was trying to get that in the billing. We can get into the ethical discussions of who that's going to target. Who's going to get taking advantage of that? That's all probably a whole class for you guys to have, or a difficult discussion.

[00:29:59.07] MARGOT KAMINSKI: In my class we talk about the benefits and costs of framing this as being property, and that's a great example of a potential way to distinguish between privacy and property. So when you're talking to constituents and they're saying privacy, privacy, privacy, what do you say about the access parts of this?

[00:30:22.14] ROBERT RODRIGUEZ: Well, I tell them-- well, I haven't seen it yet so I don't know what it's going to be like, I've barely started looking into what California is doing, as they're starting to do it. I'm excited to see what it's going to do the first, because I'm really excited to see what I'm going to ask them to-- what I'm going to ask you to provide to me. I try to tell them, the biggest enhancement for me for this bill, because it is complicated. It's so new.

[00:30:45.30] How many people in California are probably pulling their records and stuff? I'm sure there's people doing it for research and articles and stuff. The biggest thing I think that this bill does that the other states is that switch, that global privacy control. It's too complicated for anybody to know and go in. And you go read your click boxes, track cookies, this, that. this. If you just had a button that said, I don't want my stuff sold, that's the most consumer friendly tool that we can provide.

[00:31:09.91] MARGOT KAMINSKI: Yeah. This is fascinating, because you have GDPR. GDPR has various ways in which you can block the movement of data. And almost all of it-- I think Jeff was talking about this earlier-- is a standard that then gets interpreted through guidance, that then gets implemented into companies. And I remember first seeing the CCPA, and it sort of detailed description of like, you're going to have a button, it's going to say do not sell my data, it's going to appear on the front page of your website.

[00:31:40.74] I was like, oh, well, this is interesting. That's not the same. So the switch is similar, and it gets to the theme of transparency. It's about transparency is not just, let me disclose all your info, transparency is, let me make this really usable for you. So the underlying right we're trying to get at is the choice, to not give you data. But the transparency can be designed in a way that frustrates that choice, or that really enables that choice.

[00:32:08.32] ROBERT RODRIGUEZ: So it's interesting. So it's somebody who got into this and set all my cookies, turn off all my tracking apps on my phone, And I can't log into my Gmail or my Amazon anymore because it doesn't-- I have to turn on my cookies.

Which I was like that didn't used to be a thing, but somehow that's very needed for you to log in now.

[00:32:26.07] And obviously, which is a new thing for me and for the GDPR having to opt in and everything every time you click on something, I also switched to using the DuckDuckGo app on my phone which-- it works fine, I've gotten used to it. But it was really nice when my password would insert automatically and I could just do it. Well now I have to go pull up my password and have to put it in.

[00:32:47.07] And see, that's the kind of stuff. I don't know as a society in the United States that we're ready for that, and it would be very frustrating. And sometimes I get frustrated that I put myself through that, but I'm a privacy geek. I have a Facebook account and a Twitter account, I don't post my stuff because I'm the privacy guy. I just don't like-- I look at it and read it, but I don't post just because I know what they're doing.

[00:33:12.39] And it's interesting. We'll see how Elon Musk and them deal with the new thing and how they're going to sell. It They're literally saying that they're going to use it for advertising. So it'll be interesting to see the direction that goes. I be interesting to see how with reproductive health and that stuff now, with tracking and stuff next year. I've met with a lot of these organizations and was like, I don't how you guys are going to function in the United States because some states are going to tell you to block that data, and some states are going to come after you to share that data.

[00:33:36.45] Because we want to know who's going to abortion clinics. We want to know who's going with who-- the phone companies, the Ubers, the Lyfts, what are you guys going to do? I think Uber-- Lyft or somebody are getting harassed in Texas already, I think for some of this stuff. It's a new spin on privacy. Everybody's like excited to have it now These guys are going to believe in privacy well but it's going to help us go after people and do headhunting, so now we're going to do it. So it will be an interesting couple of years to see how some of this stuff plays out nationally.

[00:34:05.10] There's a lot of great apps to track this stuff. I think we've got 27, 28 states have run this bill-- tried to run an iteration of this bill and none of them have passed it, so being the third is an honor. We could have been the second had it not been COVID, but I can take that on

[00:34:22.53] MARGOT KAMINSKI: I love you're always going to hold that. Yeah, so a follow up to that and then my final question, and then I'll open up to everybody here. So my follow up to that is, you talked about how this was a bipartisan experience, and that it was almost surprising to see counterparts across the political aisle. Do you think that the characterization of data privacy in relation to reproductive rights is changing that coalition in any meaningful ways, or is there still really an bipartisan appetite for generic data privacy law?

[00:34:56.69] ROBERT RODRIGUEZ: I think generic consumer data privacy law is probably pretty broadly supported. You get into the nuance of this and I've-- so there's looks at Colorado. And I was having a conversation earlier. There's looks at doing protection, data privacy and stuff for reproductive health in the next year. And I've talked to them, and I'm like I'm happy to help, this is more complicated. , Oh no, it's not. And I was like-- No, I just don't think people should be able to get access to that data. And I was like, so what about murders, or other crimes, or terrorism, that's all protected too? And it's a very nuanced conversation when you get into legal stuff.

[00:35:31.19] And I think partisan wise, when it's legal or their sole beliefs in protecting a life, that's not going to be a concession, because it's investigating. The federal government probably has more access than I'm comfortable with. But it's about some safety and I have to be able to be OK with that balancing act. And I just hope I elect people that are smart and make sure they're protecting it, and doing and doing the right things with it.

[00:35:56.46] So I think there's a lot of good actors. The hard part with the small ones is they want to be the big ones, and they're going to use every cut to get to be a big guy. And then I think the big ones generally try to do the right thing, but it is still something that could be monetized.

[00:36:11.06] MARGOT KAMINSKI: So then my final question before I open up to you all is about the privacy impact assessment portion of the law. So again, this is a part that I was particularly excited about. It's not initially part of the California regime, it's sort of the compliance-- the boring compliance side of privacy law that actually potentially has really significant impacts in terms of how companies end up processing and mitigating the harms that arise from processing your data.

[00:36:39.15] But one thing, one feature of the Colorado Privacy Act, is that it specifically exempts privacy impact assessments from state open records laws. which means that it's envisioned as being a document that regulators can access, but not the public or third parties. And I know there's some back and forth over the regs, and how much you can get stakeholder involvement in that. But I was wondering if you could talk about that limit on transparency. What's the reasoning behind, we want these to exist, we want the information to be produced, and we don't want it to be released to the public?

[00:37:15.53] ROBERT RODRIGUEZ: Well, at the end of the day, which you get into AI some, of the directions need to be some type of impact assessment of what the decision making process is, similar to this with the data collection. And the tool is designed to help them assess their collection and to make sure there's a process that they're thinking through, what it's being utilized and not being protected? I think the unintended consequences if we made it too openly public, is if you're developing a new technology a new platform, you could be doing a

really good thorough assessment. And are you giving that proprietary information, somebody pulls it, a competitor, somebody is like, Oh well hey, now we know how he's doing everything, and we can go out and do it.

[00:37:50.94] So there has to be some type of guardrail. And maybe it's something we look at later another date, but I think there has to be some protections for people that are trying to do the right thing, and trying to develop a technology and innovation, that they have the protections to go forward, so-- which were some of the discussions we've had today with the transparency.

[00:38:06.50] MARGOT KAMINSKI: Yeah. So maybe not a transparency trade-off but a transparency paradox. Questions from the audience? So many. All right. I've got Sam, and then-- yeah.

[00:38:21.48] AUDIENCE: Hi. Thank you for speaking with us, very interesting to hear the behind the scenes. So my question is about, at the beginning, you're talking about how the Apple ask app not to track notification is really successful because it asks for what you don't want to happen, instead of making you consent to something you don't really understand

[00:38:43.95] ROBERT RODRIGUEZ: Or know.

[00:38:45.03] AUDIENCE: Yeah, and so I got that from Meg. I'm in a Professor Kaminski's class, and Meg gave us a great guest speaker presentation about why consent is basically totally flawed. But I was wondering, since like the opt-in model probably would have addressed those types of concerns, but given that that was something you had to concede, was there any other like avenues you tried to explore to accomplish something similar? And then a part 2 question is, how are you able to get the privacy or the global switch passed and not the opt-in?

[00:39:20.58] ROBERT RODRIGUEZ: Repeat the last part again.

[00:39:21.57] AUDIENCE: How are you able to get the global privacy switch passed but not the opt-in?

[00:39:27.62] ROBERT RODRIGUEZ: God. You could read a lot of articles around the country for people who chase or read privacy stuff. Probably for the corporate industry, they're probably two biggest things to fight nationally on all privacy policy is opt-in and right-of-action. And honestly, through this bill-- and I'll tell you an interesting story on one of my stakeholder meetings.

[00:39:50.69] Through this bill, having the global privacy switch was always one of the hard lines that-- like I said, we did a lot of things in the bill, and we gave and gave and gave. But it always gets to a point, like, we're not giving on a few things at the end, and we got to that at the end. The biggest fight at the end was Facebook.

[00:40:09.56] I had a stakeholder meeting, and most of the meetings are productive. And it got to the point where I'm like, just send them in writing, because you have so many different interests and so different processes that everybody was speaking over each other. So we got to a point where they'd write all their needs, and we'd go through individually-- agree, disagree, here's why, disagree.

[00:40:27.14] One of the last meetings we got to, I sat on with TechNet, another tech organization, some of the chambers who just sat there for 30 minutes telling me how the global privacy switch was an unproven technology. And it just can't be done, and other states have tried it. And it's just we've done this before. We've tried this in the past. It's just not plausible.

[00:40:46.89] And I finally ended the call with, the only plausible policy that actually does work is opt-in. So if you guys want to go with something that works, we could go with opt-in. Ended the call abruptly. They were all freaking out that I was upset.

[00:41:00.98] And then [INAUDIBLE] lobbyist had to yell at them and say, look, you can't beat the dead horse. He's not going to move on that bill. So unless you want to address everything else, you're not-- and most of the coalition and most of the legislatures, as we had conversations, understood that who can be against something that says do not sell my stuff? It's the most simplest way to do it.

[00:41:21.46] So that was the best concession I could do to opt-in, and it seems so much easier than clicking every time you go on a website. I already hate having to accept cookies, if I pull up a link on something. Next question.

[00:41:37.26] AUDIENCE: I--

[00:41:37.80] MARGOT KAMINSKI: No. Wait. One more.

[00:41:38.58] AUDIENCE: Can everyone hear me, or do we need it for the--

[00:41:40.02] MARGOT KAMINSKI: Microphone.

[00:41:40.44] ROBERT RODRIGUEZ: Here she comes.

[00:41:41.04] AUDIENCE: OK. Well, thank you very much, Senator. This has been fascinating. I'm curious, I know the process isn't done, but what do you think the costs and benefits are of this attorney general notice and comment period?

[00:42:04.22] ROBERT RODRIGUEZ: Having AG oversight is probably one of the biggest pieces in doing this kind of legislation, unless you're going to do a private right of action, which is the huger lift to do.

California's private right of action is very limited to a certain piece. The AG had to buy it. Other states, the AGs don't want to get involved.

[00:42:22.79] AG Weiser had worked on this in the Obama administration, was very knowledgeable, very engaged in wanting to do this, when we first tried to run it, the first year. So he's always been an advocate and a champion, and his team was very resourceful. And he came to me and was like, I want rule-making. And as somebody like dark pattern discussions, dark patterns wasn't even a thing when I first ran this bill, two years ago.

[00:42:45.05] It came in through an amendment, through AG Weiser's office, as we were running the bill. Could have got more detailed, but the best thought was, this technology changes so fast, I think rule-making is the best process. I was talking about cookies and running a Right to Track Bill, and I think after my bill passed, cookies are becoming a whole new technology now. So we can't legislate as fast as technology changes.

[00:43:09.29] So having rule-making and, hopefully, always a advocate in the AG's office for consumer rights is the best avenue to keep up with the tech changes, as they come. I think that was the best route we went, and I'm very lucky to have an AG who has buy-in on this process. He had a great conference on this. He brought in some people from Washington. I'm very blessed that his office is-- we're lucky in Colorado to have somebody that's passionate about consumer protections for this stuff.

[00:43:38.51] AUDIENCE: I agree.

[00:43:39.29] ROBERT RODRIGUEZ: Yeah.

[00:43:40.49] MARGOT KAMINSKI: Yeah. I'll also add to that there are some political elements of this too, where you might not be able to get consensus on a definition and the legislative process. If you have a broad term, and you're delegating it to the AG's office, that might be a different process for getting a similar definition, just to pose a hypothetical. Any other questions? All right. We have one here and here.

[00:44:06.58] ROBERT RODRIGUEZ: Quick story, while you're walking the microphone, another regret I had, which I think in the draft we had coming out of the Senate that we had to tweak out a little bit, I had taken out-- and I don't know, I assume you all know privacy. I had taken out the definition that said anonymous data, because it's just a GDPR term. It's just de-identified data. The technology is out there to re-identify this data, and you would have thought I ended the world as we know it with this policy, when I took that out.

[00:44:33.49] And I'm like, you already have de-identified. You don't need this definition. They're like, you don't under-- they practically

admitted that they use this information for that reason, which I need to follow up with the AG to make sure that's addressed in rule-making.

[00:44:46.54] [LAUGHTER]

[00:44:48.31] MARGOT KAMINSKI: [INAUDIBLE] Yeah?

[00:44:50.06] AUDIENCE: Yeah. Thank you so much for talking to us today. Could you expand on what the internal debate looked like to include nonprofits, and where you see that going? I know that Colorado is unique in the fact that it did not exclude nonprofits, and where you think that direction might head in.

[00:45:07.60] ROBERT RODRIGUEZ: Interestingly enough, I don't know if people missed nonprofits in Colorado. I always had nonprofits. For me personally, I don't understand anybody that has that amount of data, why they don't have a responsibility for protection and access. Maybe we have a discussion about the technology of releasing and not selling.

[00:45:26.86] I'm sure they sell, and they may not even know they sell. But they are, some of them, are just as gigantic as any other corporation. And I had a couple of people come to me. I think it was some insurance fraud nonprofits, and some college, school, elementary school nonprofits that collect data that were, you can't do this. No other state has nonprofits. You just need to exclude us.

[00:45:54.43] And never once did they come back to me with a solution to fix their concerns. It was just, stop doing it, and I-- because their nonprofits-- would go look up every one of their 990s and see that they were \$15, \$20, \$35 million in revenue every year, and said, you have the ability to protect this data. So I never budgeted. It never blew up.

[00:46:14.32] For me, I guess I just got lucky. We'll see if I'm lucky, in a few years. I was like, oh my God, what did I do? Because we'll see. But if we're not doing it and finding out that things are happening, then how will anybody know?

[00:46:28.47] I think Washington-- if I can find the article, I'll forward them to show it to you. But there was an article, and they taught-- every other legislator who ran this policy wished they could have had nonprofits. It's just not a fight they were willing to take on. I got lucky, or we got lucky.

[00:46:46.34] AUDIENCE: Thanks. My question is a little bit about, so you mentioned the opt-in and the private right of action were excluded, so that you could pass the bill. What were some of the conclusions that you had to, I guess, insert that you didn't want. And so the second question, this is a little bit trivial, but why the 100k limit? How did you arrive at that number?

[00:47:19.13] ROBERT RODRIGUEZ: Honestly, 100k was the same-- California has a limit too. It's just a little differently worded. It was the wording that Washington had. We're a similar sized state. It was already vetted type policy.

[00:47:32.75] The arguments, if somebody has that much record, you're going to exclude the smaller companies that are going to get caught up in this, that don't have the resources to do this work. So it was, I assume, at some point in our life, as this policy gets more-- the technology stuff will come out as people start developing things for tracking and selling and collecting data will get more beneficial for smaller ones.

[00:47:55.40] But to stifle a startup with this kind of cumbersome policy is just not feasible to do. Private right of action, for me, I think, is the most enforceable piece of legislation, because the AGs and them are probably going to go after the larger, bigger actors, because they have to invest a lot to research it. But I would rather have something rather than nothing on the books.

[00:48:17.96] MARGOT KAMINSKI: Yeah. I think, too, there's the element of-- you mentioned earlier the possibility of coordination between different states to try to harmonize between states, maybe a preemptive defense against the argument that we need federal law that's preempting.

[00:48:34.72] ROBERT RODRIGUEZ: Yeah.

[00:48:35.35] MARGOT KAMINSKI: And so those numbers being the same across different laws, I think also might be part of that effort. Any other questions from the audience? Oh, you had the second question.

[00:48:46.78] ROBERT RODRIGUEZ: We have 10 minutes.

[00:48:48.34] AUDIENCE: The inclusion of the first part [INAUDIBLE]

[00:48:56.06] ROBERT RODRIGUEZ: Well, the GDPR exclusion wording was not-- I wasn't happy with. My colleague did some exclusions for airlines and FAA's, the FAA wording, which I wasn't happy with. But United is a very big hub here, and he did it while I was with COVID in the legislature.

[00:49:15.37] So he had to carry some of the bill, and I was like in the committee. And I was like, why did you do this? He's like, we'll fix it later. Never fix it later.

[00:49:22.22] But when you work with colleagues, and you work with other people on the bill, you can't-- I have to collaborate. I can't get everything I want, and if it wouldn't have been him doing it, they would have lobbied a lot of other people to get it in the bill. And sometimes,

you have to pick and choose your battles. Every state has different nuances.

[00:49:40.22] United is a big hub here, and they had a statement and an exclusion from the court in California that got applied there too. And it was like, they'll just take it to court here. Was the fight worth doing it?

[00:49:54.63] I still read the privacy statements, when I go to the airport for United, and I'm still concerned that they're doing a lot of stuff. But it was one of those things that they case law, so that was one of my I feel bad about, and said anonymous data. I couldn't keep that out.

[00:50:10.46] MARGOT KAMINSKI: Yeah. Yeah. The United argument was a preemption argument?

[00:50:14.99] ROBERT RODRIGUEZ: It was excluding them from privacy rules, because they had a court case in California. That they went to court for California's one that said it doesn't apply to FAA.

[00:50:23.03] MARGOT KAMINSKI: Yeah.

[00:50:23.45] ROBERT RODRIGUEZ: Federal regulations.

[00:50:25.49] MARGOT KAMINSKI: Yeah. That's interesting. I see Meg.

[00:50:33.45] AUDIENCE: Thank you so much for coming. On our last panel, we talked about transparency and the historical record. And the kind of historical work that I do is everything that you are divulging to us now.

[00:50:46.86] It's so hard to get this type of insight, when we try to tell stories about how we've come to regulate computers the way that we have. So this is so valuable. It's also very entertaining, and so I really appreciate you being here.

[00:51:01.57] ROBERT RODRIGUEZ: Yeah. It was a journey. I did marry this bill, and they tell you as a legislator never to marry one, and I did marry this bill, because I was so passionate get over the thing. And like I said, it was-- it's kind of cool. I'm excited to see how it turns out in a year. I'm, like I said, honored to be a part of a policy that's transformative for people across the country and in the state and just to be part of something that's setting the trends for what could possibly be a federal law.

[00:51:30.84] AUDIENCE: Yes. Congratulations on your union.

[00:51:34.14] ROBERT RODRIGUEZ: I owe it all to my wife.

[00:51:35.61] [LAUGHTER]

[00:51:36.33] AUDIENCE: Yeah. I have a question about the global privacy switch that you are enthusiastic about. So I'm curious about how it's being designed, just how we had do not track. We've had attempts at browser-level controls, like do not track. And I think that California calls theirs global privacy.

[00:52:01.71] ROBERT RODRIGUEZ: Ours is a global privacy control as well.

[00:52:04.17] AUDIENCE: So is there-- are you continuing to pay attention to how that gets actually implemented on a technical level?

[00:52:11.88] ROBERT RODRIGUEZ: I haven't been digging in as much in the privacy stuff. I need to start digging back into the rule-making. I hadn't been-- it's an election year, and I'm up. So I haven't dug in, and like I said, I occasionally go look at the privacy websites and read stuff on it and Google the newsletters, every once in a while. I just haven't done it as much lately, because I need to look at more policy.

[00:52:32.43] Last year was just-- I didn't dig into it as much. And next year, so our bill, we put an extra year extension on it, because of the arguments I got. And it was a negotiation with the industry, when I was doing it. They're like, this is not proven.

[00:52:46.80] I go, then we'll make the rules go into effect in July of next year, but we'll do another year for the privacy control to give the AG to come up with rule-making. Who's working with other states to collaborate rule-making? But there's a lot of examples of people out there.

[00:53:00.87] One of the guys that works [INAUDIBLE] in California, is a humongous advocate for the global privacy control. So I'm confident it could be done. I just gave extra time. Because like I conceded, because I was like, look, I'll give you another year. If it's not going to happen, we can always change the law.

[00:53:21.16] So that was the avenue, but I didn't give up. Everybody's goes into effect, I think, January of this year, a lot of the other states. I conceded to the retail council, because look, it's the holiday season. We really aren't ready to gear up for this. It was a reasonable ask.

[00:53:36.00] I was like, OK, six, seven months. We're already later in the session anyway, from when the other bills passed. I was like, I don't care. Most of the states are going to conform to the tightest legislation and make it go across the country anyway.

[00:53:47.67] So the timing wasn't bad. You all see the accept cookies thing, and that's not because they're protecting our data. It's because they're doing-- it took me a while to stop going through that saying, they're not doing this for me. It's just on the website.

[00:54:00.63] MARGOT KAMINSKI: I should also just highlight, Meg is the authority on cookies in the audience. She's written a cookies book.

[00:54:07.56] ROBERT RODRIGUEZ: I was going to run a do not right to track book, right to track bill. I should have called you, and then it's all changed. It's like, yeah, cookies.

[00:54:14.79] AUDIENCE: That is the trend, though, that you're seeing across states, is they're latching on to this global privacy control.

[00:54:21.27] ROBERT RODRIGUEZ: Well, California did it before we did, but there's this only on part. Connecticut did include it. They're the last state that's passed it. Virginia did not have it. Utah did not have it.

[00:54:31.83] Some of the other states bills I snicker at. I was not happy during the process of my bill. It was always, we want you to be Virginia. We want you to be Virginia. We want you to be Virginia, and I read Virginia's.

[00:54:42.63] I was like, no. I'm not Virginia. This is Colorado. When I passed the bill, I apologized profusely, because how hard it is to get this legislation done. And I don't care what the bill, whether or not, it is not easy to get done alone, and that bill was still the second bill after California to get passed.

[00:55:02.46] So for me, pushing the envelope a little farther. Connecticut has a little bit more strength than I do. Some of the other states might have went backwards. There's a big hodgepodge of people.

[00:55:11.79] Like if we weaken this bill, and we make it stronger here, when we go federally, they're going to have all kinds of things to choose from. I hope every person that runs this policy, my only goal for them, make it better than mine. That's all I can ask.

[00:55:24.34] MARGOT KAMINSKI: Do you think there's any appetite for-- I know California did this through the ballot initiative process. But is there any appetite for going back to the CPA couple of years later, to make it-- to regulate up?

[00:55:36.03] ROBERT RODRIGUEZ: Well, it would scare the crap out of everybody, including me, because when you open Pandora's box, what can get in there. People are like, are you going to make a change? And like I said, the nonprofit would love me to exclude them.

[00:55:47.76] MARGOT KAMINSKI: Right.

[00:55:48.93] ROBERT RODRIGUEZ: Some of the other ones are looking for ways to run a bill, and I said, if you don't have buy-in from us and the AG, it's going to be harder, but whatever. Everybody gets to try to run their bills. I haven't seen a reason-- or the AG has not come

back to me to say we need to do physical changes to the policy, to lead me to go in and do it. I'd like to start looking at AI, biometrics.

[00:56:11.61] We start talking about meta and virtual worlds, and now you have your eyeballs getting scanned, and you're looking at stuff. And now they see how your eyes open and dilate when you're looking at things, and who knows what's going to come out of that. And those are the things we need to start getting ahead of. It's too late for data privacy, for what we've done. It just got ahead of us.

[00:56:32.10] We've got to start thinking ahead for more rules for them. And I think these assessments and stuff, it puts accountabilities on them to think through. Because they're excited to do any technology to do it, but nobody-- I don't think-- they're not as responsible to think through the unintended consequences of what they're doing. And that's where we need to step in and say-- I don't think we need to do super regulate, but you need to write down something of what you're doing and why, so at least you have something to refer to.

[00:56:58.93] MARGOT KAMINSKI: Yeah. One of the things that has been coming up in conversations around AI policy, recently, is just the notion of AI snake oil. Right? That there's not a whole lot out there to say-- you're in trouble if you promote an AI system as being able to do something, and it turns out it can't. It turns out it's bad. It doesn't function.

[00:57:19.96] So very excited to continue these conversations with you. Thank you so much for joining us. You'd all join me in thanking Senator Rodriguez.

[00:57:27.12] [APPLAUSE]